

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

Авторы-составители: **Лунегов Игорь Владимирович**

Программа производственной практики
ПРОИЗВОДСТВЕННАЯ ПРАКТИКА
Код УМК 97485

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

Пермь, 2021

1. Вид практики, способ и форма проведения практики

Вид практики **производственная**

Тип практики **практика по получению профессиональных умений и опыта профессиональной деятельности**

Способ проведения практики **стационарная, выездная**

Форма (формы) проведения практики **дискретная**

2. Место практики в структуре образовательной программы

Производственная практика « Производственная 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 :

Целью практики является закрепление и углубление теоретических знаний полученных в ходе учебного процесса (лекционных и практических занятий), приобретение практических навыков и компетенций, а также опыта самостоятельной профессиональной деятельности.

Задачи практики :

- приобретение практических навыков работы с системами защиты информации;
- приобретение практических навыков работы с алгоритмами программного обеспечения систем защиты информации;
- приобретение практических навыков по настройке оборудования по защите информации;
- приобретение практических навыков работы по анализу технологий построения современных систем защиты информации;
- сбор информации от оборудования по защите информации;
- систематизация полученных данных с целью подготовки отчета;
- изучение нормативных и методических документов по вопросам расчетно-проектной деятельности при построении системы защиты информации;
- определение перспективных направлений развития технологий информационной безопасности;

3. Перечень планируемых результатов обучения

В результате прохождения практики **Производственная 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.10.1 Разрабатывает техническую документацию на компоненты автоматизированных систем

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.11.2 Разрабатывает и администрирует базы данных

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.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.3 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

Индикаторы

ОПК.3.2 Применяет на практике знание нормативных правовых актов, нормативных и методически документов, регламентирующих деятельность по защите информации

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

ОПК.9 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Индикаторы

ОПК.9.3 Применяет методы и средства криптографической защиты информации для решения профессиональных задач

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

ПК.2 Способен выбирать и моделировать архитектурные решения для реализации интегрированного программного обеспечения

Индикаторы

ПК.2.1 Определяет перечень элементов архитектуры, которые должны быть защищены от угроз безопасности информации

ПК.3 Способен управлять функционированием и защищенностью автоматизированных систем

Индикаторы

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

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

ПК.4 Способен оценивать уровень безопасности компьютерных систем и сетей

Индикаторы

ПК.4.3 Определяет уровень защищенности и доверия программно-аппаратных средств защиты информации

ПК.5 Способен анализировать уязвимости внедряемой системы защиты информации

Индикаторы

ПК.5.1 Проводит анализ уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы

ПК.5.2 Проводит экспертизы состояния защищенности информации автоматизированных систем

ПК.6 Способен проводить контроль защищенности информации от утечки по техническим каналам

Индикаторы

ПК.6.3 Проводит контроль защищенности информации от несанкционированного доступа и специальных воздействий

4. Содержание и объем практики, формы отчетности

Производственная 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.

Специальность	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
форма обучения	очная
№№ триместров, выделенных для прохождения практики	15,16
Объем практики (з.е.)	15
Объем практики (ак.час.)	540
Форма отчетности	Экзамен (15 триместр) Экзамен (16 триместр)

Примерный график прохождения практики

Количество часов	Содержание работ	Место проведения
Производственная практика. Первый учебный период.		
432	Производственная 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", обладающей необходимым кадровым и научно-техническим потенциалом. Производственная практика предназначена для получения практических навыков работы, связанных с защитой информации организации.	Предприятия и организации, с которыми заключен договор о практической подготовке
Вводный инструктаж		
6	Вводный инструктаж проводится на кафедре радиоэлектроники и защиты информации. После прибытия на место практики студенты должны пройти инструктаж на рабочем месте.	Кафедра радиоэлектроники и защиты информации, а также предприятия и организации, с которыми заключен договор о практической подготовке
Знакомство со структурой организации		
20	Изучение структуры предприятия, назначения и основных производственных функций подразделений предприятия.	Предприятия и организации, с которыми заключен договор о практической подготовке
Изучение организации труда на предприятии		

Количество часов	Содержание работ	Место проведения
20	Изучение основных обязанностей должностных лиц подразделения по вопросам организации защиты информации.	Предприятия и организации, с которыми заключен договор о практической подготовке
Решение поставленной профессиональной задачи		
366	Решение практической или теоретической задачи в области обеспечения информационной безопасности, связанной с работой организации.	Предприятия и организации, с которыми заключен договор о практической подготовке
Подготовка и сдача промежуточного отчета по производственной практике		
20	Подготовка предварительного отчета о результатах производственной практики	Кафедра радиоэлектроники и защиты информации
Производственная практика. Второй учебный период.		
108		
Завершающий этап решения поставленной профессиональной задачи.		
90	Решение практической или теоретической задачи в области обеспечения информационной безопасности, связанной с работой организации. Подготовка рекомендаций об улучшении информационной безопасности на предприятии и/или выполнение обязанностей в соответствии должностными инструкциями.	Предприятия и организации, с которыми заключен договор о практической подготовке
Подготовка и сдача итогового отчета по производственной практике		
18	Подготовка окончательного отчета о результатах производственной практики	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. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. <https://www.urait.ru/bcode/511998>
2. Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов : Ай Пи Ар Букс, 2015. — 326 с. — ISBN 978-5-906-17271-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/33857>

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

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

<http://www.fsb.ru> Официальный сайт ФСБ России
<https://fstec.ru> Официальный сайт ФСТЭК России
<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 **Производственная практика** предполагает использование следующего программного обеспечения и информационных справочных систем:

В ходе производственной практики могут быть использованы следующие информационные технологии:

- презентационные материалы;
 - 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».

А также используются информационные технологии, предоставляемые предприятиями по месту проведения практики студентов.

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

Практика проводится с использованием материально-технического обеспечения, предоставляемого предприятиями по месту проведения практики студентов.

При освоении материала и выполнении заданий по дисциплине рекомендуется использование материалов, размещенных в личных кабинетах обучающихся ЕТИС ПГНИУ (student.psu.ru). Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся: При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.
2. Система видеоконференцсвязи на основе платформы BigBlueButton (<https://bigbluebutton.org/>).
3. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
4. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
5. Система тестирования Indigo (<https://indigoes.ru/>).
6. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.
7. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
8. 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

Для успешного прохождения производственной 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.

Для обучающихся с ОВЗ производственная практика проводится с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья (далее – индивидуальные особенности). При прохождении практики 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 практики 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
ОПК.14.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	сформированные знания требований безопасности автоматизированных систем, сформированные умения разрабатывать политики информационной безопасности автоматизированных систем, сформированные навыки реализации политики информационной безопасности автоматизированных систем	Неудовлетворительно не знает требований безопасности автоматизированных систем, не умеет разрабатывать политики информационной безопасности автоматизированных систем, не владеет навыками их реализации Удовлетворительно 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 Хорошо 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 Отлично сформированные знания требований безопасности автоматизированных систем, сформированные умения разрабатывать политики информационной безопасности автоматизированных систем, сформированные навыки реализации политики информационной безопасности

		Отлично автоматизированных систем
--	--	---

ОПК.3

Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.3.2 Применяет на практике знание нормативных правовых актов, нормативных и методически документов, регламентирующих деятельность по защите информации	знать нормативно-методические материалы по проведению испытаний, уметь анализировать результаты измерений, полученных техническими средствами, владеть навыками использования специализированного оборудования для проведения испытаний	<p>Неудовлетворительно не знает нормативно-методические материалы по проведению испытаний, не умеет анализировать результаты измерений, полученных техническими средствами, не владеет навыками использования специализированного оборудования для проведения испытаний</p> <p>Удовлетворительно частично сформированные знания нормативно-методические материалы по проведению испытаний, частично сформированные умения анализировать результаты измерений, полученных техническими средствами, частично сформированные навыки использования специализированного оборудования для проведения испытаний</p> <p>Хорошо сформированные, но содержащие пробелы знания нормативно-методические материалы по проведению испытаний, сформированные, но содержащие пробелы умения анализировать результаты измерений, полученных техническими средствами, сформированные, но содержащие пробелы навыки использования специализированного оборудования для проведения испытаний</p> <p>Отлично сформированные знания нормативно-методические материалы по проведению испытаний, сформированные умения анализировать результаты измерений, полученных техническими средствами, сформированные навыки использования специализированного оборудования для проведения испытаний</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
ОПК.16.1 Осуществляет обоснованный выбор технологий, инструментария, языка программирования и способов оптимизации программ	знать методологии и методы проектирования программного обеспечения, уметь работать с интегрированной средой разработки программного обеспечения, владеть навыками тестирования программ в интегрированной среде разработки.	<p>Неудовлетворительно 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>Удовлетворительно 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>Хорошо 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>Отлично сформированное знание методологии и методов проектирования программного обеспечения, сформированное умение работать с интегрированной средой разработки программного обеспечения, сформированные навыки тестирования программ в интегрированной среде разработки.</p>

ОПК.11

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

ОПК.11.1 Компетенция Оценивает (индикатор) эффективность и	Планируемые результаты обучения владеет навыками анализа защищенности информационной системы с	Критерии оценивания результатов обучения Неудовлетворительно не владеет навыками анализа защищенности информационной системы с использованием
надежность защиты операционных систем	использованием специализированного оборудования	Удовлетворительно специализированного оборудования частично сформированные навыки анализа защищенности информационной системы с использованием специализированного оборудования Хорошо сформированные, но содержащие пробелы навыки анализа защищенности информационной системы с использованием специализированного оборудования Отлично сформированные навыки анализа защищенности информационной системы с использованием специализированного оборудования
ОПК.11.2 Разрабатывает и администрирует базы данных	знать современные СУБД, уметь проектировать реляционные базы данных, владеть навыками администрирования баз данных	Неудовлетворительно не знает современные СУБД, не умеет проектировать реляционные базы данных, не владеет навыками администрирования баз данных Удовлетворительно частично сформированные знания современных СУБД, частично сформированное умение проектировать реляционные базы данных, посредственное владение навыками администрирования баз данных Хорошо сформированные, но содержащие пробелы знания современных СУБД, сформированное, но содержащие пробелы умение проектировать реляционные базы данных, неуверенное владение навыками администрирования баз данных Отлично сформированные знания современных СУБД, сформированное умение проектировать реляционные базы данных, уверенное владение навыками администрирования баз данных

ОПК.10

Способен разрабатывать компоненты систем защиты информации автоматизированных систем

ОПК.10.2 Компетенция Проектирует защищенные (индикатор)	знать средства защиты Планируемые результаты информации и средств обучения контроля защищенности	Неудовлетворительно Критерии оценивания результатов не знает средства защиты информации и средств контроля защищенности обучения
автоматизированные системы с учетом действующих нормативных и методических документов	автоматизированной системы, уметь проектировать средства защиты информации и средства контроля защищенности автоматизированной системы, владеть навыками настройки и оптимизации действующих средств защиты информации	автоматизированной системы, не умеет проектировать средства защиты информации и средства контроля защищенности автоматизированной системы, не владеет навыками настройки и оптимизации действующих средств защиты информации Удовлетворительно 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 Хорошо 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 Отлично 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
ОПК.10.1 Разрабатывает техническую документацию на компоненты	знать состав структурных компонентов автоматизированных систем, владеть навыками разработки структурных компонентов	Неудовлетворительно отсутствие знания состава структурных компонентов автоматизированных систем, отсутствие навыков разработки структурных компонентов автоматизированных систем

автоматизированных систем	автоматизированных систем	<p>Удовлетворительно частично сформированные знания состава структурных компонентов автоматизированных систем, частичное владение навыками разработки структурных компонентов автоматизированных систем</p> <p>Хорошо сформированные, но содержащие пробелы знания состава структурных компонентов автоматизированных систем, в целом успешное, но содержащее отдельные пробелы применение навыков разработки структурных компонентов автоматизированных систем</p> <p>Отлично сформированные знания состава структурных компонентов автоматизированных систем, успешное и систематическое применение навыков разработки структурных компонентов автоматизированных систем</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>ОПК.6.3 Применяет методы и приемы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей</p>	Знать основные принципы проведения научных исследований, уметь ставить и решать задачи, владеть навыками исследовательской деятельности	<p>Неудовлетворительно не знает основные принципы проведения научных исследований, не умеет ставить и решать задачи, не владеет навыками исследовательской деятельности</p> <p>Удовлетворительно частично сформированные знания основных принципов проведения научных исследований, частично сформированные умения ставить и решать задачи, частично сформированные навыки исследовательской деятельности</p> <p>Хорошо 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>Отлично</p>

		<p>Отлично</p> <p>сформированные знания основных принципов проведения научных исследований, сформированные умения ставить и решать задачи, сформированные навыки исследовательской деятельности</p>
--	--	--

ОПК.9

Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ОПК.9.3</p> <p>Применяет методы и средства криптографической защиты информации для решения профессиональных задач</p>	<p>владеть навыками контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств</p>	<p>Неудовлетворительно</p> <p>не владеет навыками контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств</p> <p>Удовлетворительно</p> <p>частично сформированные навыки контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств</p> <p>Хорошо</p> <p>сформированные, но содержащие пробелы навыки контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств</p> <p>Отлично</p> <p>сформированные навыки контроля защищенности автоматизированной системы с помощью технических, программно-аппаратных и криптографических средств</p>

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ОПК.4.3</p> <p>Организует защиту информации ограниченного доступа</p>	<p>знать нормативно-правовую базу в области защиты информации, уметь разрабатывать методические</p>	<p>Неудовлетворительно</p> <p>не знает нормативно-правовую базу в области защиты информации, не умеет разрабатывать методические материалы по</p>

<p>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</p>	<p>материалы по обслуживанию систем безопасности информационной системы, владеть навыками оценки и контроля полноты содержания нормативных и методических материалов</p>	<p>Неудовлетворительно обслуживанию систем безопасности информационной системы, не владеет навыками оценки и контроля полноты содержания нормативных и методических материалов</p> <p>Удовлетворительно 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>Хорошо 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>Отлично сформированные знания нормативно-правовой базы в области защиты информации, сформированные умения разрабатывать методические материалы по обслуживанию систем безопасности информационной системы, сформированные навыки оценки и контроля полноты содержания нормативных и методических материалов</p>
--	--	--

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ОПК.13.2 Оценивает эффективность и</p>	<p>знать политики информационной безопасности организации, уметь</p>	<p>Неудовлетворительно не знает политики информационной безопасности организации, не умеет</p>

надежность средств защиты информации программного обеспечения автоматизированных систем	контролировать эффективность политики информационной безопасности организации, владеть навыками формирования правил, обеспечивающих информационную безопасность предприятия	<p>Неудовлетворительно контролировать эффективность политики информационной безопасности организации, не владеет навыками формирования правил, обеспечивающих информационную безопасность предприятия</p> <p>Удовлетворительно частично сформированные знания политики информационной безопасности организации, фрагментарные умения контролировать эффективность политики информационной безопасности организации, частично сформированные навыки формирования правил, обеспечивающих информационную безопасность предприятия</p> <p>Хорошо сформированные, но содержащие пробелы знания политики информационной безопасности организации, сформированные, но содержащие пробелы умения контролировать эффективность политики информационной безопасности организации, сформированные, но содержащие пробелы навыки формирования правил, обеспечивающих информационную безопасность предприятия</p> <p>Отлично сформированные знания политики информационной безопасности организации, сформированные умения контролировать эффективность политики информационной безопасности организации, сформированные навыки формирования правил, обеспечивающих информационную безопасность предприятия</p>
---	---	--

ОПСК.3

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПСК.3.1 Обнаруживает и устраняет нарушения правил разграничения доступа в автоматизированных	знать правила, процедуры, практические приемы, руководящие принципы, методы, средства для обеспечения информационной безопасности АС, уметь	<p>Неудовлетворительно не знает правила, процедуры, практические приемы, руководящие принципы, методы, средства для обеспечения информационной безопасности автоматизированной системы, не умеет формировать и эффективно</p>

системах	формировать и эффективно применять комплекс мер для обеспечения информационной безопасности АС	<p>Неудовлетворительно применять комплекс мер для обеспечения информационной безопасности автоматизированной системы</p> <p>Удовлетворительно 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>Хорошо 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>Отлично 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 автоматизированной системы</p>
ОПСК.3.2 Определяет источники и причины возникновения инцидентов безопасности в автоматизированных системах	Знать возможные пути вторжений в АС, владеть навыками защиты информационной системы от внешних вторжений	<p>Неудовлетворительно не знает возможные пути вторжений в АС, не владеет навыками защиты информационной системы от внешних вторжений</p> <p>Удовлетворительно частично сформированные знания возможных путей вторжений в АС, частично сформированные навыки защиты АС от внешних вторжений</p> <p>Хорошо сформированные, но содержащие пробелы знания возможных путей вторжений в АС,</p>

		<p>Хорошо сформированные, но содержащие пробелы навыки защиты АС от внешних вторжений</p> <p>Отлично сформированные знания возможных путей вторжений в АС, сформированные навыки защиты АС от внешних вторжений</p>
--	--	---

ОПСК.1

Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ОПСК.1.2 Проводит сбор, систематизацию и оценку сведений об угрозах безопасности информации, оценивает необходимость защиты информации, формулирует требования к защите информации</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>Неудовлетворительно 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>Удовлетворительно 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>Хорошо 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>Отлично сформированные знания требований предъявляемых к информационной безопасности предприятия</p>

		<p>Отлично</p> <p>безопасности предприятия, сформированные умения устанавливать, настраивать и обслуживать средства информационной безопасности предприятия, сформированные навыки совершенствования существующих систем информационной безопасности предприятия</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>ПК.1.3</p> <p>Анализирует эффективность решений по обеспечению информационной безопасности автоматизированных систем</p>	<p>Знать составляющие системы защиты информации в автоматизированных системах. Уметь оценивать эффективность системы защиты информации в автоматизированных системах. Владеть методами оценки эффективности системы защиты информации в автоматизированных системах.</p>	<p>Неудовлетворительно</p> <p>Не способен оценивать эффективность системы защиты информации в компьютерных системах.</p> <p>Удовлетворительно</p> <p>Частично сформированные знания составляющих системы защиты информации в автоматизированных системах. Частично сформированное умение оценивать эффективность системы защиты информации в автоматизированных системах. Посредственное владение методами оценки эффективности системы защиты информации в автоматизированных системах.</p> <p>Хорошо</p> <p>Сформированные, но содержащие пробелы знания составляющих системы защиты информации в автоматизированных системах. Сформированное, но содержащие пробелы умение оценивать эффективность системы защиты информации в автоматизированных системах. Неуверенное владение методами оценки эффективности системы защиты информации в автоматизированных системах.</p> <p>Отлично</p> <p>Сформированные знания составляющих системы защиты информации в автоматизированных системах. Сформированное умение оценивать эффективность системы защиты</p>

		<p>Отлично</p> <p>информации в автоматизированных системах. Уверенное владение методами оценки эффективности системы защиты информации в автоматизированных системах.</p>
--	--	--

ПК.3

Способен управлять функционированием и защищенностью автоматизированных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.3.1</p> <p>Контролирует соответствие параметров подсистем защиты автоматизированной системы установленным требованиям</p>	<p>Знать компоненты системы защиты информации предприятия и подсистемы информационной безопасности автоматизированной системы. Уметь контролировать состояние подсистемы информационной безопасности автоматизированной системы.</p>	<p>Неудовлетворительно</p> <p>Не знает компоненты системы защиты информации предприятия и подсистемы информационной безопасности автоматизированной системы. Не умеет контролировать состояние подсистемы информационной безопасности автоматизированной системы.</p> <p>Удовлетворительно</p> <p>Частично сформированные знания компонент системы защиты информации предприятия и подсистемы информационной безопасности автоматизированной системы. Частично сформированное умение контролировать состояние подсистемы информационной безопасности автоматизированной системы.</p> <p>Хорошо</p> <p>Сформированные, но содержащие пробелы знания компонент системы защиты информации предприятия и подсистемы информационной безопасности автоматизированной системы. Сформированное, но содержащие пробелы умение контролировать состояние подсистемы информационной безопасности автоматизированной системы.</p> <p>Отлично</p> <p>Сформированные знания компонент системы защиты информации предприятия и подсистемы информационной безопасности автоматизированной системы. Сформированное умение контролировать состояние подсистемы информационной безопасности автоматизированной системы.</p>
<p>ПК.3.3</p> <p>Проводит мероприятия</p>	<p>Знать перечень мероприятий, проводимых при аттестации</p>	<p>Неудовлетворительно</p> <p>Не знает перечень мероприятий,</p>

<p>по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД</p>	<p>объектов требованиям информационной безопасности, владеть навыками проведения мероприятий по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД</p>	<p>Неудовлетворительно проводимых при аттестации объектов требованиям информационной безопасности, не владеет навыками проведения мероприятий по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД</p> <p>Удовлетворительно Частично сформированные знания перечня мероприятий, проводимых при аттестации объектов требованиям информационной безопасности, посредственное владение навыками проведения мероприятий по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД</p> <p>Хорошо Сформированные, но содержащие пробелы знания перечня мероприятий, проводимых при аттестации объектов требованиям информационной безопасности, неуверенное владение навыками проведения мероприятий по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД</p> <p>Отлично Сформированные знания перечня мероприятий, проводимых при аттестации объектов требованиям информационной безопасности, уверенное владение навыками проведения мероприятий по аттестации на предмет соответствия требованиям по защите сооружений и автоматизированных систем от НСД</p>
--	--	--

ПК.2

Способен выбирать и моделировать архитектурные решения для реализации интегрированного программного обеспечения

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.2.1 Определяет перечень элементов архитектуры, которые должны быть защищены от угроз безопасности</p>	<p>знать виды угроз и модели нарушителя информационной безопасности автоматизированной системы, уметь разрабатывать модели угроз и модели нарушителя</p>	<p>Неудовлетворительно отсутствие знания видов угроз и моделей нарушителя информационной безопасности автоматизированной системы, отсутствие умения разрабатывать модели угроз и модели нарушителя информационной</p>

информации	информационной безопасности автоматизированной системы, владеть навыками формирования перечня и вероятности угроз информационной безопасности	<p>Неудовлетворительно безопасности автоматизированной системы, отсутствие навыков формирования перечня и вероятности угроз информационной безопасности</p> <p>Удовлетворительно 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>Хорошо 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>Отлично 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>
------------	---	--

ПК.4

Способен оценивать уровень безопасности компьютерных систем и сетей

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.4.3 Определяет уровень	владеть навыками анализа защищенности	Неудовлетворительно не владеет навыками анализа защищенности

защищенности и доверия программно-аппаратных средств защиты информации	информационной системы с использованием специализированного оборудования	<p>Неудовлетворительно информационной системы с использованием специализированного оборудования</p> <p>Удовлетворительно частично сформированные навыки анализа защищенности информационной системы с использованием специализированного оборудования</p> <p>Хорошо сформированные, но содержащие пробелы навыки анализа защищенности информационной системы с использованием специализированного оборудования</p> <p>Отлично сформированные навыки анализа защищенности информационной системы с использованием специализированного оборудования</p>
--	--	---

ПК.5

Способен анализировать уязвимости внедряемой системы защиты информации

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.5.1 Проводит анализ уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы	Уметь определять уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы	<p>Неудовлетворительно Не умеет определять уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы</p> <p>Удовлетворительно Частично сформированное умение определять уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы</p> <p>Хорошо Сформированное, но содержащие пробелы умение определять уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы</p> <p>Отлично Сформированное умение определять уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы</p>
ПК.5.2 Проводит экспертизы состояния	знать систему управления информационной безопасностью	<p>Неудовлетворительно не знает систему управления информационной безопасностью</p>

защищенности информации автоматизированных систем	автоматизированных систем, уметь проводить анализ защищенности автоматизированных систем и предлагать решения по их совершенствованию	<p>Неудовлетворительно автоматизированных систем, не умеет проводить анализ защищенности автоматизированных систем и предлагать решения по их совершенствованию</p> <p>Удовлетворительно частично сформированные знания системы управления информационной безопасностью автоматизированной системы, частично сформированные умения проводить анализ защищенности автоматизированных систем и предлагать решения по их совершенствованию</p> <p>Хорошо сформированные, но содержащие пробелы знания системы управления информационной безопасностью автоматизированной системы, сформированные, но содержащие пробелы умения проводить анализ защищенности автоматизированных систем и предлагать решения по их совершенствованию</p> <p>Отлично сформированные знания системы управления информационной безопасностью автоматизированной системы, сформированные умения проводить анализ защищенности автоматизированных систем и предлагать решения по их совершенствованию</p>
---	---	--

ПК.6

Способен проводить контроль защищенности информации от утечки по техническим каналам

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.6.3 Проводит контроль защищенности информации от несанкционированного доступа и специальных воздействий	Знать технические средства, применяемые при проведении специальных воздействий на автоматизированные системы, владеть навыками контроля защищенности информации от несанкционированного доступа и специальных воздействий	<p>Неудовлетворительно Не знает технические средства, применяемые при проведении специальных воздействий на автоматизированные системы, не владеет навыками контроля защищенности информации от несанкционированного доступа и специальных воздействий</p> <p>Удовлетворительно Частично сформированные знания технических средств, применяемых при проведении специальных воздействий на автоматизированные системы,</p>

		<p>Удовлетворительно посредственное владение навыками контроля защищенности информации от несанкционированного доступа и специальных воздействий</p> <p>Хорошо Сформированные, но содержащие пробелы знания технических средств, применяемых при проведении специальных воздействий на автоматизированные системы, неуверенное владение навыками контроля защищенности информации от несанкционированного доступа и специальных воздействий</p> <p>Отлично Сформированные знания технических средств, применяемых при проведении специальных воздействий на автоматизированные системы, уверенное владение навыками контроля защищенности информации от несанкционированного доступа и специальных воздействий</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.	Неудовлетворительно
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.	Удовлетворительно
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.	Хорошо
Оценивается работа студента, выполнившего весь объем работы, определенной программой практики, проявившего теоретическую	Отлично

подготовку и умелое применение полученных знаний в ходе практики, оформившего документы практики, отчет в соответствии со всеми требованиями и защитивший его.	Отлично
--	----------------

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.	Неудовлетворительно
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.	Удовлетворительно
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.	Хорошо
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.	Отлично