

МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

Авторы-составители: Лунегов Игорь Владимирович

Программа учебной практики

НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА

Код УМК 94120

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

Пермь, 2021

1. Вид практики, способ и форма проведения практики

Вид практики **учебная**

Тип практики **практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности**

Способ проведения практики **стационарная, выездная**

Форма (формы) проведения практики **дискретная**

2. Место практики в структуре образовательной программы

Учебная практика « Научно-исследовательская работа » 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 НИР является развитие интеллектуальных способностей студентов путем изучения ими алгоритма научного исследования и приобретения начального опыта выполнения исследовательского проекта на учебном материале по специальности Информационная безопасность автоматизированных систем

Задачи практики :

1. Овладение навыками самостоятельной постановки научно-исследовательских задач, а также планирование натурного и вычислительного экспериментов.
2. Овладение навыками поиска научных литературных источников, содержащих необходимую для научной работы информацию.
3. Научиться самостоятельно, проводить экспериментальные и теоретические исследования с использованием современного оборудования и имеющихся программных пакетов.
4. Овладеть навыками статистической обработки полученных результатов и составления научного отчета о проделанной работе.
5. Аккумулировать материалы для подготовки диссертационного исследования, научных публикаций в рамках магистерской научно-исследовательской работы;
6. Развить культуру оформления результатов научных исследований как важнейшее условие успешного решения задач будущей профессиональной деятельности.

3. Перечень планируемых результатов обучения

В результате прохождения практики **Научно-исследовательская работа** у обучающегося должны быть сформированы следующие компетенции:

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

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.15.2 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.16.2 Использует языки высокого и низкого уровня, технологии программирования, методы и инструментальные средства для решения профессиональных, исследовательских и прикладных задач

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.5 Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ

Индикаторы

ОПК.5.1 Создаёт программы на языках высокого и низкого уровня, применяет методы и инструментальные средства программирования для решения профессиональных задач

ОПК.5.2 Осуществляет обоснованный выбор инструментария программирования и способов организации программ

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

Индикаторы

ОПК.6.1 Ориентируется в методах и приемах научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

ОПК.6.2 Осуществляет выбор необходимых методов и приемов научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

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

ОПК.7 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

Индикаторы

ОПК.7.1 Ориентируется в методах и средствах защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методах и средствах защиты информации от утечки по техническим каналам, сетей и систем передачи информации

ОПК.7.2 Применяет методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации при решении профессиональных задач, учитывая текущее состояние и тенденции развития методов и средств обеспечения защиты информации

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

Индикаторы

ОПСК.1.1 Использует средства операционных систем для обеспечения безопасного функционирования автоматизированных систем

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

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.1.2 Использует языки, системы, инструментальные, программные и аппаратные средства, методы моделирования для испытаний систем защиты

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.2.2 Разрабатывает архитектуры программного обеспечения интегрированной программной системы, в соответствии с требованиями конфиденциальности, целостности и доступности

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.3.2 Осуществляет перевод текстов с иностранного языка на русский и с русского на иностранный в академических и профессиональных целях

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

4. Содержание и объем практики, формы отчетности

Научно-исследовательская работа в триместре проводится для закрепления и углубления теоретических знаний, сбора и обработки материала для написания выпускной квалификационной работы, приобретения обучающимся практических навыков в научно-исследовательской работе, а также навыков самостоятельной работы в научно-исследовательском коллективе.

| | |
|---|--|
| Специальность | 10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем) |
| форма обучения | очная |
| №№ триместров, выделенных для прохождения практики | 9 |
| Объем практики (з.е.) | 3 |
| Объем практики (ак.час.) | 108 |
| Форма отчетности | Зачет (9 триместр) |

Примерный график прохождения практики

| Количество часов | Содержание работ | Место проведения |
|--|---|--|
| Научно-исследовательская работа | | |
| 108 | Научно-исследовательская работа студентов является составной частью основной образовательной программы высшего образования и представляет собой форму организации учебного процесса, непосредственно ориентированную на развитие исследовательских навыков у учащихся. Научно-исследовательская работа может проводиться 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 | Местами прохождения практики могут быть учебные и учебно-научные лаборатории, а также компьютерный класс кафедры радиоэлектроники и защиты информации, оснащенные оборудованием, указанным в паспортах и позволяющим выполнить весь комплекс работ по тематике исследований. |
| Установочные занятия | | |
| 14 | Постановка задач на выполнение научно-исследовательской работы. Получение заданий от руководителя. Согласование плана выполнения работ. | Кафедра радиоэлектроники и защиты информации, Научная библиотека ПГНИУ с доступом к локальной и глобальной сети Интернет |
| Обзор литературы | | |
| 24 | Данный этап НИР посвящен анализу литературы по теме | Кафедра радиоэлектроники |

| Количество часов | Содержание работ | Место проведения |
|---|---|--|
| | исследований. Должен в обязательном порядке включать изучение периодических изданий как на русском, так и английском языках. | и защиты информации, Научная библиотека ПГНИУ с доступом к локальной и глобальной сети Интернет |
| Анализ и обобщение данных | | |
| 28 | На данном этапе осуществляется анализ и обобщение данных, полученных в ходе изучения литературы. Результатом анализа должно стать заключение (выводы) о состоянии современной науки и техники в исследуемой области. | Кафедра радиоэлектроники и защиты информации, Научная библиотека ПГНИУ с доступом к локальной и глобальной сети Интернет |
| Составление отчета и подготовка презентации | | |
| 24 | На данном этапе формируется отчет о проделанной работе и готовится презентация. | Кафедра радиоэлектроники и защиты информации, Научная библиотека ПГНИУ с доступом к локальной и глобальной сети Интернет |
| Защита НИР | | |
| 18 | Завершающий этап НИР предназначен для оформления результатов исследования. Студентом готовится презентация для защиты. На защиту студент должен представить презентацию и отзыв руководителя НИР, подтверждающий объем выполненной работы и готовность студента к защите. | Кафедра радиоэлектроники и защиты информации, Научная библиотека ПГНИУ с доступом к локальной и глобальной сети Интернет |

5. Перечень учебной литературы, необходимой для проведения практики

Основная

1. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — Москва : СОЛОН-Пресс, 2018. — 262 с. — ISBN 978-5-91359-173-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. <http://www.iprbookshop.ru/90375>
2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2019. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // ЭБС Юрайт [сайт]. <https://www.urait.ru/bcode/447581>
3. Современные радиоэлектронные средства и технологии информационной безопасности : монография / В. А. Майстренко, А. А. Соловьев, М. Ю. Пляскин, А. И. Тихонов. — Омск : Омский государственный технический университет, 2017. — 356 с. — ISBN 978-5-8149-2554-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/78508.html>

Дополнительная

1. Комплексное обеспечение информационной безопасности автоматизированных систем : лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш [и др.]. — Ставрополь : Северо-Кавказский федеральный университет, 2016. — 242 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/62945.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>
3. Технические средства и методы защиты информации: учебное пособие для студентов вузов, обучающихся по специальностям 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммуникационных систем" / А. П. Зайцев [и др.] ; ред.: А. П. Зайцев, А. А. Шелупанов. -4-е изд., испр. и доп..-Москва:Горячая линия - Телеком,2012, ISBN 978-5-9912-0084-4.-616.- Библиогр.: с. 608-609

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

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

<http://dlib.eastview.com/browse> Электронная база данных научных периодических изданий

<http://e.lanbook.com> Издательство Лань

<http://www.intuit.ru> Научная и методическая IT-литература

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

7. Перечень информационных технологий, используемых при проведении практики

Образовательный процесс по практике **Научно-исследовательская работа** предполагает использование следующего программного обеспечения и информационных справочных систем:

Образовательный процесс по дисциплине предполагает использование следующего информационных технологий, программного обеспечения и информационных справочных систем:

- 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 (ЕТИС ПГНИУ);
- 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 используемого программного обеспечения:

- открытая система "ALT Linux"
- офисный пакет приложений "Libre office";
- приложение позволяющее просматривать и воспроизводить медиа контент PDF-файлов "Adobe Acrobat Reader DC";
- программы демонстрации видео материалов (проигрыватель) "Windows Media Plaer";

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в личных кабинетах обучающихся ЕТИС ПГНИУ (etis.pgu.ru).

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

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

Материально-техническая база обеспечивается наличием:

1. Лекционные занятия, занятия семинарского типа (семинары, практические занятия), групповые (индивидуальные) консультации, мероприятия текущего контроля и промежуточной аттестации проводятся в аудитории, оснащенной презентационной техникой (проектор, экран для проектора, компьютер/ноутбук), а также меловой (и) или маркерной доской.

2. Самостоятельная работа

система тестирования Indigo (<https://indigotech.ru/>).
Аудитория для самостоятельной работы, в том числе помещения Научной библиотеки ПГНИУ, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченные доступом в электронную информационно-образовательную среду университета.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера 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

Научно-исследовательская работа является одним из этапов написания ВКР студентом, по завершении которого у студента уже должна быть сформирована основа (черновик) его будущей работы. Для успешного выполнения НИР 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.

Отчет представляет собой законченную разработку, в котором 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.

Темы научно-исследовательских работ для студентов:

1. Дискреционный доступ и методы его реализации.
2. Многоуровневый доступ и методы его реализации.
3. Базовые методы обеспечения безопасности (контроль повторного использования объектов, анализ тайных каналов передачи информации, протоколирование и аудит системы защиты).
4. Основные элементы и принципы работы системы безопасности в UNIX и Windows.

5. Структура файловой системы и средства обеспечения безопасности в NTFS.
6. Структура файловой системы и средства обеспечения безопасности в ext3 и ext4.
7. Процедура загрузки ОС Linux. Процесс Init и конфигурационные файлы.
8. Назначение, структура и редактирование файла /etc/fstab.
9. Linux-PAM. Основные возможности и настройка.
10. SELinux. Структура, возможности и настройка.
11. Основные разновидности компьютерных вирусов и средств защиты.
12. Криптографические методы защиты информации и их применение в современных ОС.
13. Базовые принципы построения систем обнаружения вторжений.
14. Мониторы виртуальных машин. Назначение, аппаратная поддержка и реализация.
15. Виртуальная память и средства ее поддержки.
16. Нейронные сети и их применение в обеспечения безопасности.
17. Методы разграничения доступа. Понятие матрицы доступа.
18. Понятие информационной безопасности. Безопасные системы и угрозы безопасности. Роль операционных систем в обеспечении информационной безопасности.
19. Методы повышения производительности файловых систем. Структура и принципы работы буферного пула в UNIX.
20. Алгоритмы выполнения системных вызовов open, read, write и close в операционной системе UNIX.
21. Логическая структура файловой системы. Монтирование файловых систем в UNIX.
22. Особенности устройства процессора, работающего в режиме мультипрограммирования.
23. Базовые принципы управления памятью.
24. Аппаратно-программные средства управления внешними устройствами в мультипрограммной среде.
25. Методы доступа к файлам, их особенности и реализация.
26. Схемы памяти с фиксированным и переменным числом разделов: общие принципы, связывание адресов, обеспечение достаточного объема и защита памяти.
27. Управление памятью в операционной системе UNIX и вспомогательные структуры данных.
28. Подкачка страниц и средства ее поддержки. Модель рабочего множества и ее использование для организации замещения страниц в многозадачной среде.
29. Принципы реализации процессов. Блок управления процессом и его состав в UNIX.
30. Алгоритмы выполнения системных вызовов fork, exec и exit в UNIX.
31. Методы обеспечения надежности файловых систем. Сохранение и восстановление целостности.

Для обучающихся с ОВЗ научно-исследовательская работа может выполняться с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья (далее – индивидуальные особенности). При выполнении научно-исследовательской работы 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 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.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 |
|---|---|---|
| ОПК.6.1 Ориентируется в методах и приемах научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей | знает основные требования при проведении научных экспериментов, умеет обрабатывать результаты измерений, владеет навыками работы с измерительными приборами | <p style="text-align: center;">Неудовлетворительно</p> не знает основные требования при проведении научных экспериментов, не умеет обрабатывать результаты измерений, не владеет навыками работы с измерительными приборами <p style="text-align: center;">Удовлетворительно</p> частично сформированные знания основных требований при проведении научных экспериментов, частично сформированные умения обрабатывать результаты измерений, частично сформированные навыки работы с измерительными приборами <p style="text-align: center;">Хорошо</p> сформированные, но содержащие пробелы знания основных требований при проведении научных экспериментов, сформированные, но содержащие пробелы знания умения обрабатывать результаты измерений, сформированные, но содержащие пробелы знания навыки работы с измерительными приборами <p style="text-align: center;">Отлично</p> сформированные знания основных требований при проведении научных экспериментов, сформированные умения обрабатывать результаты измерений, сформированные навыки работы с измерительными приборами |
| ОПК.6.2 Осуществляет выбор необходимых методов и приемов научных исследований при проведении разработок в области обеспечения безопасности | Знать основные принципы проведения научных исследований, уметь ставить и решать задачи, владеть навыками исследовательской деятельности | <p style="text-align: center;">Неудовлетворительно</p> не знает основные принципы проведения научных исследований, не умеет ставить и решать задачи, не владеет навыками исследовательской деятельности <p style="text-align: center;">Удовлетворительно</p> частично сформированные знания основных принципов проведения научных |

| | | |
|---|---|---|
| компьютерных систем и сетей | | <p>Удовлетворительно 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 сформированные знания основных принципов проведения научных исследований, сформированные умения ставить и решать задачи, сформированные навыки исследовательской деятельности</p> |
| <p>ОПК.6.3 Применяет методы и приемы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей</p> | <p>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</p> | <p>Неудовлетворительно 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</p> <p>Удовлетворительно 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</p> <p>Хорошо сформированные, но содержащие пробелы знания основных требований информационной безопасности, предъявляемые к АС, сформированные, но содержащие пробелы умения организовать разработку, внедрение, эксплуатацию и</p> |

| | | |
|--|--|---|
| | | <p>Хорошо сопровождение автоматизированной системы с учетом требований информационной безопасности, сформированные, но содержащие пробелы навыки администрирования компьютерной сети предприятия</p> <p>Отлично сформированные знания основных требований информационной безопасности, 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.7

Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|--|--|
| <p>ОПК.7.1 Ориентируется в методах и средствах защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методах и средствах защиты информации от утечки по техническим каналам, сетей и систем передачи информации</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>Неудовлетворительно не знает оборудования, используемого при проведении экспериментально-исследовательских работ по сертификации средств защиты автоматизированных систем, не умеет выбирать необходимое оборудование при проведении экспериментально-исследовательских работ, не владеет навыками использования специализированных средств при анализе технических каналов утечки информации</p> <p>Удовлетворительно 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,</p> |

| | | |
|---|---|---|
| | | <p>Удовлетворительно</p> <p>частично</p> <p>сформированные навыки использования специализированных средств при анализе технических каналов утечки информации</p> <p>Хорошо</p> <p>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>Отлично</p> <p>сформированные знания видов оборудования, используемого при проведении экспериментально-исследовательских работ по сертификации средств защиты автоматизированных систем, сформированные умения выбирать необходимое оборудование при проведении экспериментально-исследовательских работ, сформированные навыки использования специализированных средств при анализе технических каналов утечки информации</p> |
| <p>ОПК.7.2</p> <p>Применяет методы и средства защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методы и средства защиты информации от утечки по техническим каналам, сетей и систем передачи информации при решении профессиональных задач, учитывая</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>Неудовлетворительно</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>Удовлетворительно</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</p> |

| | | |
|---|--|---|
| <p>текущее состояние и тенденции развития методов и средств обеспечения защиты информации</p> | | <p>Удовлетворительно</p> <p>ОИС</p> <p>Хорошо</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>Отлично</p> <p>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 ОИС</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>ОПК.16.2</p> <p>Использует языки высокого и низкого уровня, технологии программирования, методы и инструментальные средства для решения профессиональных, исследовательских и прикладных задач</p> | <p>Знать основные языки программирования, уметь использовать программные средства в профессиональной деятельности, владеть навыками разработки ПО</p> | <p>Неудовлетворительно</p> <p>Знать основные языки программирования, уметь использовать программные средства в профессиональной деятельности, владеть навыками разработки ПО</p> <p>Удовлетворительно</p> <p>Знать основные языки программирования, уметь использовать программные средства в профессиональной деятельности, владеть навыками разработки ПО</p> <p>Хорошо</p> <p>Знать основные языки программирования, уметь использовать программные средства в профессиональной деятельности, владеть навыками разработки ПО</p> <p>Отлично</p> <p>Знать основные языки программирования, уметь использовать программные средства в</p> |

| | | |
|---|------------------------------------|---|
| | | Отлично профессиональной деятельности, владеть навыками разработки ПО |
| ОПК.16.1 Осуществляет обоснованный выбор технологий, инструментария, языка программирования и способов оптимизации программ | знать способы оптимизации программ | Неудовлетворительно не знает способы оптимизации программ Удовлетворительно Частично сформированные знания способов оптимизации программ Хорошо Сформированные, но содержащие пробелы знания способов оптимизации программ Отлично Сформированные знания способов оптимизации программ |

ОПК.5

Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|---|--|
| ОПК.5.2 Осуществляет обоснованный выбор инструментария программирования и способов организации программ | Уметь выбирать инструментарии программирования и способы организации программ | Неудовлетворительно Не умеет выбирать инструментарии программирования и способы организации программ Удовлетворительно Частично сформированное умение выбирать инструментарии программирования и способы организации программ Хорошо Сформированное, но содержащие пробелы умение выбирать инструментарии программирования и способы организации программ Отлично Сформированное умение выбирать инструментарии программирования и способы организации программ |
| ОПК.5.1 Создаёт программы на языках высокого и низкого уровня, применяет методы и инструментальные средства программирования для | владеть навыками разработки структурных компонентов автоматизированных систем | Неудовлетворительно Отсутствие навыков разработки структурных компонентов автоматизированных систем Удовлетворительно Частичное владение навыками разработки структурных компонентов автоматизированных систем Хорошо |

| | | |
|--------------------------------|--|---|
| решения профессиональных задач | | <p>Хорошо</p> <p>В целом успешное, но содержащее отдельные пробелы применение навыков разработки структурных компонентов автоматизированных систем</p> <p>Отлично</p> <p>Успешное и систематическое применение навыков разработки структурных компонентов 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>ОПК.15.2</p> <p>Применяет знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач</p> | <p>Знать физические принципы возникновения каналов утечки информации, уметь анализировать процессы, происходящие в автоматизированных системах, владеть навыками идентификации возможных каналов утечки информации</p> | <p>Неудовлетворительно</p> <p>Не знает физические принципы возникновения каналов утечки информации, не умеет анализировать процессы, происходящие в автоматизированных системах, не владеет навыками идентификации возможных каналов утечки информации</p> <p>Удовлетворительно</p> <p>Частично сформированные знания физических принципов возникновения каналов утечки информации. Частично сформированные умения анализировать процессы, происходящие в автоматизированных системах. Посредственное владение навыками идентификации возможных каналов утечки информации</p> <p>Хорошо</p> <p>Сформированные, но содержащие пробелы знания физических принципов возникновения каналов утечки информации. Сформированные, но содержащие пробелы умения анализировать процессы, происходящие в автоматизированных системах. Неуверенное владение навыками идентификации возможных каналов утечки информации</p> <p>Отлично</p> <p>Сформированные знания физических принципов возникновения каналов утечки</p> |

| | | |
|--|--|--|
| | | <p style="text-align: center;">Отлично</p> <p>информации. Сформированные умения анализировать процессы, происходящие в автоматизированных системах. Уверенное владение навыками идентификации возможных каналов утечки информации</p> |
|--|--|--|

ОПК.17

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

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|--|---|
| <p>ОПК.17.2 Ориентируясь на задачи профессиональной деятельности, обоснованно выбирает информационно-коммуникационные технологии и использует их в профессиональной деятельности с учетом требований информационной безопасности</p> | <p>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> | <p style="text-align: center;">Неудовлетворительно</p> <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> <p style="text-align: center;">Удовлетворительно</p> <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> <p style="text-align: center;">Хорошо</p> <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> <p style="text-align: center;">Отлично</p> <p>сформированные знания программных и</p> |

| | | |
|--|--|--|
| | | <p>Отлично</p> <p>программно-аппаратных средств используемых для защиты информационной системы, сформированные умения настраивать программные и аппаратные средства защиты, сформированные навыки администрирования подсистемы информационной безопасности автоматизированной системы</p> |
|--|--|--|

ОПСК.1

Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|--|--|--|
| <p>ОПСК.1.1</p> <p>Использует средства операционных систем для обеспечения безопасного функционирования автоматизированных систем</p> | <p>Знать технологии обеспечения безопасности автоматизированных систем, уметь настраивать систему безопасности операционной системы, владеть навыками системного администрирования</p> | <p>Неудовлетворительно</p> <p>Не знает технологии обеспечения безопасности автоматизированных систем, не умеет настраивать систему безопасности операционной системы, не владеет навыками системного администрирования</p> |
| | | <p>Удовлетворительно</p> <p>Частично сформированные знания технологий обеспечения безопасности автоматизированных систем, частично сформированное умение настраивать систему безопасности операционной системы, посредственное владение навыками системного администрирования</p> |
| | | <p>Хорошо</p> <p>Сформированные, но содержащие пробелы знания технологий обеспечения безопасности автоматизированных систем, сформированное, но содержащие пробелы умение настраивать систему безопасности операционной системы, неуверенное владение навыками системного администрирования</p> |
| | | <p>Отлично</p> <p>Сформированные знания технологий обеспечения безопасности автоматизированных систем, сформированное умение настраивать систему безопасности операционной системы, уверенное владение навыками системного администрирования</p> |

| | | |
|--|--|---|
| <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 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> | <p>Неудовлетворительно 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>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> |
|--|--|---|

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 |
|---|--|---|
| ПК.1.3 Анализирует эффективность решений по обеспечению информационной безопасности автоматизированных систем | 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>Неудовлетворительно 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>Удовлетворительно 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>Хорошо 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>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 ОИС</p> |
| ПК.1.2 Использует языки, системы, инструментальные, программные и аппаратные средства, | Знать особенности построения автоматизированных систем, уметь строить модели автоматизированных систем, владеть навыками разработки моделей автоматизированных | <p>Неудовлетворительно отсутствие знания особенностей построения автоматизированных систем, отсутствие умения строить модели автоматизированных систем, отсутствие навыки разработки моделей автоматизированных систем</p> |

| | | |
|---|--|---|
| <p>методы моделирования для испытаний систем защиты</p> | <p>систем</p> | <p>Удовлетворительно частично сформированные знания особенностей построения автоматизированных систем, частично сформированные умения строить модели автоматизированных систем, частично сформированные навыки разработки моделей автоматизированных систем</p> <p>Хорошо 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>Отлично сформированные знания особенностей построения автоматизированных систем, сформированные умения строить модели автоматизированных систем, сформированные навыки разработки моделей автоматизированных систем</p> |
| <p>ПК.1.1 Проводит моделирование безопасности информационных систем</p> | <p>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> | <p>Неудовлетворительно 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>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</p> |

| | | |
|--|--|---|
| | | <p>Хорошо</p> <p>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</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> |
|--|--|---|

ПК.2

Способен выбирать и моделировать архитектурные решения для реализации интегрированного программного обеспечения

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|---|---|
| ПК.2.1 Определяет перечень элементов архитектуры, которые должны быть защищены от угроз безопасности информации | Знать критерии оценки защищенности автоматизированных систем, уметь проводить анализ защищенности автоматизированных систем, владеть навыками использования программных и аппаратных средств для защиты информации в АС | <p>Неудовлетворительно</p> <p>не знает критериев оценки защищенности автоматизированных систем, не умеет проводить анализ защищенности автоматизированных систем, не владеет навыками использования программных и аппаратных средств для защиты информации в АС</p> <p>Удовлетворительно</p> <p>частично сформированные знания критериев оценки защищенности автоматизированных систем, частично сформированные умения проводить анализ защищенности автоматизированных систем, частично сформированные навыки использования программных и аппаратных средств для защиты информации в АС</p> <p>Хорошо</p> |

| | | |
|--|--|---|
| | | <p>Хорошо сформированные, но содержащие пробелы знания критериев оценки защищенности автоматизированных систем, сформированные, но содержащие пробелы умения проводить анализ защищенности автоматизированных систем, сформированные, но содержащие пробелы навыки использования программных и аппаратных средств для защиты информации в АС</p> <p>Отлично сформированные знания критериев оценки защищенности автоматизированных систем, сформированные умения проводить анализ защищенности автоматизированных систем, сформированные навыки использования программных и аппаратных средств для защиты информации в АС</p> |
| <p>ПК.2.2 Разрабатывает архитектуры программного обеспечения интегрированной программной системы, в соответствии с требованиями конфиденциальности, целостности и доступности</p> | <p>владеть навыками разработки защищенной автоматизированной системы в заданном исполнении</p> | <p>Неудовлетворительно Отсутствие навыков разработки защищенной автоматизированной системы</p> <p>Удовлетворительно Фрагментарное применение навыков разработки защищенной автоматизированной системы в заданном исполнении</p> <p>Хорошо В целом успешное, но содержащее отдельные пробелы навыков разработки защищенной автоматизированной системы в заданном исполнении</p> <p>Отлично Успешное и систематическое применение навыков разработки защищенной автоматизированной системы в заданном исполнении</p> |

УК.3

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

| Компетенция (индикатор) | Планируемые результаты обучения | Критерии оценивания результатов обучения |
|---|--|--|
| <p>УК.3.1 Осуществляет коммуникацию, грамотно и аргументированно</p> | <p>знать грамматику одного из иностранных языков, уметь поддерживать диалог на иностранном языке, владеть навыками представления</p> | <p>Неудовлетворительно не знает грамматику одного из иностранных языков, не умеет поддерживать диалог на иностранном языке, не владеет навыками технического перевода</p> |

| | | |
|--|---|--|
| <p>строит устную и письменную речь на русском и иностранном языках</p> | <p>информации на иностранном языке</p> | <p>Удовлетворительно частично сформированные знания грамматики одного из иностранных языков, частично сформированные умения поддерживать диалог на иностранном языке, частично сформированные навыки технического перевода</p> <p>Хорошо 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>Отлично сформированные знания грамматики одного из иностранных языков, сформированные умения поддерживать диалог на иностранном языке, сформированные навыки технического перевода</p> |
| <p>УК.3.2 Осуществляет перевод текстов с иностранного языка на русский и с русского на иностранный в академических и профессиональных целях</p> | <p>знает правила правописания одного из иностранных языков, умеет читать и осуществлять перевод технической документации, владеет навыками разговорного общения</p> | <p>Неудовлетворительно знает правила правописания одного из иностранных языков, умеет читать и осуществлять перевод технической документации, владеет навыками разговорного общения</p> <p>Удовлетворительно знает правила правописания одного из иностранных языков, умеет читать и осуществлять перевод технической документации, владеет навыками разговорного общения</p> <p>Хорошо знает правила правописания одного из иностранных языков, умеет читать и осуществлять перевод технической документации, владеет навыками разговорного общения</p> <p>Отлично знает правила правописания одного из иностранных языков, умеет читать и осуществлять перевод технической документации, владеет навыками разговорного общения</p> |
| <p>УК.3.3 Представляет</p> | <p>знать основные требования к подготовке презентации на</p> | <p>Неудовлетворительно не знает основные требования к подготовке</p> |

| | | |
|--|--|--|
| <p>результаты деятельности на публичных мероприятиях в устной и письменной формах</p> | <p>публичных мероприятиях, уметь пользоваться презентационной техникой, владеть навыками использования приложений для подготовки презентаций</p> | <p>Неудовлетворительно презентации на публичных мероприятиях, не умеет пользоваться презентационной техникой, не владеет навыками использования приложений для подготовки презентаций</p> <p>Удовлетворительно частично сформированные знания основных требований к подготовке презентации на публичных мероприятиях, частично сформированные умения пользоваться презентационной техникой, частично сформированные навыки использования приложений для подготовки презентаций</p> <p>Хорошо 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>Отлично сформированные знания основных требований к подготовке презентации на публичных мероприятиях, сформированные умения пользоваться презентационной техникой, сформированные навыки использования приложений для подготовки презентаций</p> |
| <p>УК.3.4 Устанавливает и поддерживает контакты в академическом и профессиональном взаимодействии с использованием современных коммуникативных технологий</p> | <p>Знать способы формирования контактов в научном сообществе, уметь налаживать контакты с коллегами в сфере профессиональной деятельности, владеть навыками использования современных коммуникативных технологий для взаимодействия в профессиональной сфере</p> | <p>Неудовлетворительно Знать способы формирования контактов в научном сообществе, уметь налаживать контакты с коллегами в сфере профессиональной деятельности, владеть навыками использования современных коммуникативных технологий для взаимодействия в профессиональной сфере</p> <p>Удовлетворительно Знать способы формирования контактов в научном сообществе, уметь налаживать контакты с коллегами в сфере профессиональной деятельности, владеть навыками использования современных коммуникативных технологий для взаимодействия в профессиональной сфере</p> <p>Хорошо</p> |

| | | |
|--|--|--|
| | | <p>Хорошо</p> <p>Знать способы формирования контактов в научном сообществе, уметь налаживать контакты с коллегами в сфере профессиональной деятельности, владеть навыками использования современных коммуникативных технологий для взаимодействия в профессиональной сфере</p> <p>Отлично</p> <p>Знать способы формирования контактов в научном сообществе, уметь налаживать контакты с коллегами в сфере профессиональной деятельности, владеть навыками использования современных коммуникативных технологий для взаимодействия в профессиональной сфере</p> |
|--|--|--|

Оценочные средства

Вид мероприятия промежуточной аттестации : Зачет

Способ проведения мероприятия промежуточной аттестации : Защищаемое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации :
время отводимое на доклад 4

Показатели оценивания

| | |
|---|------------------|
| Ставится за недостаточно полный объем навыков и компетенции в рамках программы практики. Неумение использовать в практической деятельности научную терминологию, изложение ответов на вопросы с существенными стилистическими и логическими ошибками. Слабое владение инструментарием учебных дисциплин по разделам программы практики, некомпетентность в решении стандартных (типовых) учебных задач. Невыполнение индивидуального задания, пассивность при выполнении поручений, низкий уровень культуры исполнения заданий, | Незачтено |
| Ставится за систематизированные, глубокие и полные навыки и компетенции по всем разделам программы НИР. Использование научной терминологии, стилистически грамотное, логически правильное изложение ответов на вопросы, умение делать обоснованные выводы. Владение инструментарием учебных дисциплин, умение эффективно использовать его в решении поставленных задач. Способность самостоятельно и творчески решать сложные проблемы в нестандартных учебных ситуациях. Полное выполнение индивидуального задания. | Зачтено |