МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

Авторы-составители: **Лунегов Игорь Владимирович**

Программа производственной практики

ПРОИЗВОДСТВЕННАЯ ПРАКТИКА

Код УМК 81677

Утверждено
Протокол №4
от «24» июня 2020 г.

Пермь, 2020

1. Вид практики, способ и форма проведения практики

Вид практики **производственная**
Тип практики **профессиональная – практика, направленная на приобретение 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 Блок « С.2 » образовательной программы по направлениям подготовки (специальностям):

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

Цель практики :

Целью прохождения производственной практики является изучение опыта создания и применения защищенных информационных технологий и систем для решения реальных задач организационной, управленческой или научной деятельности в условиях конкретных производств, организаций или корпораций; приобретение навыков практического решения задач защиты информации на рабочем месте.

Задачи практики :

Задачи практики:
- углубление знаний, полученных в ходе обучения, развитие навыков их применения в практической области защиты информации;
- расширение представлений о функциональных возможностях защищенных информационных систем;
- усвоение и закрепление навыков самостоятельной работы и самостоятельного решения поставленных задач;
- сбор материала для последующего его использования при изучении учебных дисциплин;
- углубление практических умений и навыков по профессиональной деятельности в рамках направления "Информационная безопасность";
- формирование умения анализировать и оценивать свою собственную профессиональную деятельность.

Данные задачи соотносятся со следующими видами профессиональной деятельности и их задачами:
эксплуатационная деятельность:
- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации;
- администрирование подсистем информационной безопасности объекта;

проектно-технологическая деятельность:
- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- участие в разработке технологической и эксплуатационной документации.

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 (специализация : Безопасность открытых информационных систем)

ОК.3 способность работать самостоятельно и в коллективе, уметь находить и принимать организационно-управленческие решения, оценивать их эффективность

ОПК.4 готовность к участию в проведении научных исследований

ОПК.7 способность применять нормативные правовые акты в профессиональной деятельности

ПК.1 способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности, в том числе на иностранном языке

ПК.2 способность осваивать и применять современные программные технические средства и методы исследования с использованием компьютерных технологий

ПК.3 способность разрабатывать и исследовать модели автоматизированных систем

ПК.33 способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности

ПК.4 способность проводить анализ защищенности автоматизированных систем

ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы

ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем

ПК.8 способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ

ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем

ПСК.1.1 способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем

ПСК.1.2 способность разрабатывать и реализовывать политики информационной безопасности открытых информационных систем

ПСК.1.3 способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы

ПСК.1.4 способность участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы

ПСК.1.5 способность формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем

4. Содержание и объем практики, формы отчетности

Настоящая программа производственной практики составлена для студентов специальности «Информационная безопасность автоматизированных систем» с учетом СУОС, учебного плана, календарного графика учебного процесса.

Направления подготовки	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
форма обучения	очная
№№ триместров, выделенных для прохождения практики	12
Объем практики (з.е.)	12
Объем практики (ак.час.)	432
Форма отчетности	Экзамен (12 триместр)

Примерный график прохождения практики

Количество часов	Содержание работ	Место проведения
Производственная практика [КРиЗИ]. Первый семестр		
432		Производственная практика проводится в лабораториях кафедры радиоэлектроники и защиты информации, лабораториях и подразделениях Пермского госуниверситета, научно-исследовательских институтах, ведущих конструкторских, проектных бюро, производственных предприятиях и объединениях. Места прохождения практики определяются решением кафедры радиоэлектроники и защиты информации. Направление студентов на практику в другие организации производится в соответствии с

Количество часов	Содержание работ	Место проведения
		заключенными договорами.
Подготовительный этап		
16	Подготовительный этап предполагает общее собрание студентов, уходящих на практику, на котором проводится инструктаж по технике безопасности при работе в исследовательских лабораториях и на месте прохождения практики, обсуждается общий план работы студента на все время практики, определяются и закрепляются руководители практики за каждым студентом.	Подготовительный этап проходит в ПГНИУ на кафедре радиоэлектроники и защиты информации
Основной этап		
400	На основном этапе прохождения практики студенты изучают структуры подразделения - места прохождения практики, знакомятся с организационной структурой отдела (подразделения) защиты информации, основными приемами и методами защиты информации данного подразделения, нормативно-правовой документацией предприятия по обеспечению информационной безопасности, законодательно-правовой базой по защите персональных данных сотрудников подразделения. Осуществляется сбор материала для анализа ситуаций нарушения информационной безопасности, если таковые имеются, анализируются возможные уязвимости предприятия (организации), выполняются работы по научно-исследовательской деятельности в области защиты информации. Выполняются установки, настройки или эксплуатации компонентов системы обеспечения информационной безопасности согласно индивидуальным задачам производственной практики.	Основной этап практики проходит по месту прохождения - в лабораториях кафедры радиоэлектроники и защиты информации, лабораториях и подразделениях Пермского госуниверситета, научно-исследовательских институтах, ведущих конструкторских, проектных бюро, производственных предприятиях и объединениях.
Завершающий этап		
16	На завершающем этапе производственной практики студенты оформляют отчет о проделанной за время практики работе. Отчет должен содержать: 1. Введение, включающее в себя цели и задачи практики, а также объект исследования, раскрывается основное содержание практики, отображается значение и актуальность выбранной темы. 2. В основную часть отчета должны быть включены данные, отражающие сущность и основные результаты выполненной работы во время практики. 3. В заключении подводится итог всей выполненной работы	Завершающий этап проходит в ПГНИУ на кафедре 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 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/87995.html

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. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю. Н. Сычев. — Саратов : Вузовское образование, 2018. — 195 c. — ISBN 978-5-4487-0128-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/72345.html

Дополнительная

1. Никитина Е. Ю.,Черников А. В. Рекомендации по написанию выпускной квалификационной работы в области информационной безопасности:учебно-методическое пособие/Е. Ю. Никитина, А. В. Черников.-Пермь:ПГНИУ,2019.-27. https://elis.psu.ru/node/603259

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. https://urait.ru/bcode/451933

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

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

http://uisrussia.msu.ru Университетская информационная система «Россия»
http://www.knigafund.ru/ Электронная библиотечная система «КнигаФонд»
http://e.lanbook.com/ Электронная библиотечная система издательства «Лань»
https://habr.com/ru/hub/infosecurity/ Информационная безопасность
https://softline.ru/solutions/security Сайт компании Softline
https://www.smart-soft.ru/blog/informatsionnaja-bezopasnost/ Сайт компании Смарт-софт

7. Перечень информационных технологий, используемых при проведении практики

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

- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной 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";

Специализированное программное обеспечение по защите информации

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

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

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

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

система тестирования Indigo (https://indigotech.ru/).

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

Используется приборный парк учебных, учебно-научных и научных лабораторий кафедры радиоэлектроники и защиты информации, а также оборудование на предприятиях по месту прохождения производственной практики

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 освоению дисциплины

Производственная практика является одним из этапов написания ВКР студентом, по завершении которого у студента уже должна быть сформирована основа (черновик) его будущей работы. Для успешного прохождения практики необходимо:

- обсуждение индивидуального плана прохождения практики с научным руководителем;
- перед началом практики участвовать в организационно-инструктивных собраниях с группой студентов-практикантов;
- выразить свое желание по выбору предприятия, учреждения и конкретного руководителя, сообщив об этом ответственному за прохождение практики;
- изучать и строго соблюдать правила охраны труда, техники безопасности и производственной санитарии;
- прислушаться советам руководителя от кафедры радиоэлектроники и защиты информации;
- подчиняться действующим на предприятии, в учреждении правилам внутреннего трудового распорядка;
- стараться полностью выполнять задания, предусмотренные индивидуальным планом;
- наравне со штатными работниками нести ответственность за выполненную работу и ее результаты;
- своевременно сообщать научному руководителю о непредвиденных препятствиях, трудностях при выполнении индивидуального плана работы;
- вести дневник, где записывать необходимые цифровые материалы, содержание лекций и бесед, делать эскизы, зарисовки, схемы и т.д.;
- отзыв индивидуального руководителя (в соответствующем месте дневника или в виде отдельного документа) должен быть передан на кафедру радиоэлектроники и защиты информации.

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 /ets/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 е 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 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 дисциплине для формирования компетенции и критерии их оценивания

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.4 готовность к участию в проведении научных исследований	Знать основные особенности научного подхода, уметь применять методологию научных исследований, владеть навыками критического восприятия информации	**Неудовлетворительно** отсутствие знаний основных особенностей научного подхода, отсутствие умения применять методологию научных исследований, отсутствие навыков критического восприятия информации **Удовлетворительно** Частично сформированные знания основных особенностей научного подхода, частично сформированные умения применять методологию научных исследований, частично сформированные навыки критического восприятия информации **Хорошо** Сформированные, но содержащие пробелы знания основных особенностей научного подхода, сформированные, но содержащие пробелы умения применять методологию научных исследований, сформированные, но содержащие пробелы навыки критического восприятия информации **Отлично** Полностью сформированные знания основных особенностей научного подхода, сформированные умения применять методологию научных исследований, сформированные навыки критического восприятия информации
ПСК.1.1 способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных	знать типы нормативных документов, относящихся к безопасности информации предприятия, уметь составлять документы, определяющие безопасность информации на предприятии	**Неудовлетворительно** не знает нормативных документов, относящихся к безопасности информации предприятия, не умеет составлять документы, определяющие безопасность информации на предприятии **Удовлетворительно** Частично сформированные знания типов нормативных документов, относящихся к безопасности информации предприятия,

систем		**Удовлетворительно** частично сформированные умения составлять документы, определяющие безопасность информации на предприятии **Хорошо** Сформированные, но содержащие пробелы знания типов нормативных документов, относящихся к безопасности информации предприятия, сформированные, но содержащие пробелы умения составлять документы, определяющие безопасность информации на предприятии **Отлично** Полностью сформированные знания типов нормативных документов, относящихся к безопасности информации предприятия, сформированные умения составлять документы, определяющие безопасность информации на предприятии
ПК.2 способность осваивать и применять современные программные технические средства и методы исследования с использованием компьютерных технологий	знать современные технические средства для защиты информации и уметь применять их на практике, владеть навыками исследования с использованием компьютерных технологий	**Неудовлетворительно** не знает современные технические средства для защиты информации и не умеет применять их на практике, не владеет навыками исследования с использованием компьютерных технологий **Удовлетворительно** частично сформированные знания современных технических средств для защиты информации, частично сформированное умение применять современные технические средства для защиты информации, посредственное владение навыками исследования с использованием компьютерных технологий **Хорошо** сформированные, но содержащие пробелы знания современных технических средств для защиты информации, сформированное, но содержащие пробелы умение применять современные технические средства для защиты информации, неуверенное владение навыками исследования с использованием компьютерных технологий **Отлично** Полностью сформированные знания современных технически средств для защиты информации и умение применять их на практике, уверенное владение навыками

		Отлично исследования с использованием компьютерных технологий
ПК.1 способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности, в том числе на иностранном языке	знать хотя бы один иностранный язык, уметь осуществлять поиск необходимой научно-технической информации, владеть навыками составления реферативных обзоров	**Неудовлетворительно** не знает ни одного иностранного языка, не умеет осуществлять поиск необходимой научно-технической информации, не владеет навыками составления реферативных обзоров **Удовлетворительно** частично сформированные знания английского языка, частично сформированное умение осуществлять поиск необходимой научно-технической информации, посредственное владение навыками составления реферативных обзоров **Хорошо** сформированные, но содержащие пробелы знания иностранного языка, сформированное, но содержащие пробелы умение осуществлять поиск необходимой научно-технической информации, неуверенное владение навыками составления реферативных обзоров **Отлично** Полностью сформированные знания хотя бы одного иностранного языка, сформированное умение осуществлять поиск необходимой научно-технической информации, уверенное владение навыками составления реферативных обзоров
ПК.33 способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере	знать основы электроники и схемотехники, уметь читать радиоэлектронные схемы, владеть навыками схемотехнического моделирования	**Неудовлетворительно** не знает основ электроники и схемотехники, не умеет читать радиоэлектронные схемы, не владеет навыками схемотехнического моделирования **Удовлетворительно** частично сформированные знания основ электроники и схемотехники, частично сформированное умение читать радиоэлектронные схемы, посредственное владение навыками схемотехнического моделирования **Хорошо** сформированные, но содержащие пробелы знания основ электроники и схемотехники, сформированное, но содержащие пробелы

профессиональной деятельности		**Хорошо** умение читать радиоэлектронные схемы, неуверенное владение навыками схемотехнического моделирования **Отлично** полностью сформированные знания основ электроники и схемотехники, сформированное умение читать радиоэлектронные схемы, уверенное владение навыками схемотехнического моделирования
ОПК.7 способность применять нормативные правовые акты в профессиональной деятельности	знать иерархию нормативных документов, уметь применять нормативные правовые акты при составлении правил использования автоматизированных систем	**Неудовлетворительно** не знает иерархию нормативных документов, не умеет применять нормативные правовые акты при составлении правил использования автоматизированных систем **Удовлетворительно** частично сформированные знания иерархии нормативных документов, частично сформированное умение применять нормативные правовые акты при составлении правил использования автоматизированных систем **Хорошо** сформированные, но содержащие пробелы знания иерархии нормативных документов, сформированное, но содержащие пробелы умение применять нормативные правовые акты при составлении правил использования автоматизированных систем **Отлично** полностью сформированные знания иерархии нормативных документов, сформированное умение применять нормативные правовые акты при составлении правил использования автоматизированных систем
ПК.4 способность проводить анализ защищенности автоматизированных систем	знать методы поиска уязвимости автоматизированных систем, уметь проводить анализ защищенности автоматизированных систем	**Неудовлетворительно** не знает методов поиска уязвимости автоматизированных систем, не умеет проводить анализ защищенности автоматизированных систем **Удовлетворительно** частично сформированные знания методов поиска уязвимости автоматизированных систем, частично сформированное умение проводить анализ защищенности

		Удовлетворительно автоматизированных систем **Хорошо** сформированные, но содержащие пробелы знания методов поиска уязвимости автоматизированных систем, сформированное, но содержащие пробелы умение проводить анализ защищенности автоматизированных систем **Отлично** полностью сформированные знания методов поиска уязвимости автоматизированных систем, сформированное умение проводить анализ защищенности автоматизированных систем
ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы	Знать место анализа рисков в общей системе обеспечения информационной безопасности, уметь оценивать информационные риски в автоматизированных системах, владеть методами количественной и качественной оценки информационных рисков	**Неудовлетворительно** не знает место анализа рисков в общей системе обеспечения информационной безопасности, не умеет оценивать информационные риски в автоматизированных системах, не владеет методами количественной и качественной оценки информационных рисков **Удовлетворительно** частично сформированное знание места анализа рисков в общей системе обеспечения информационной безопасности, частично сформированное умение оценивать информационные риски в автоматизированных системах, посредственное владение методами количественной и качественной оценки информационных рисков **Хорошо** сформированное, но содержащее пробелы знание места анализа рисков в общей системе обеспечения информационной безопасности, сформированное, но содержащее пробелы умение оценивать информационные риски в автоматизированных системах, неуверенное владение методами количественной и качественной оценки информационных рисков **Отлично** Полностью сформированное знание места анализа рисков в общей системе обеспечения информационной безопасности,

		Отлично сформированное умение оценивать информационные риски в автоматизированных системах, уверенное владение методами количественной и качественной оценки информационных рисков
ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем	уметь проводить анализ защищенности автоматизированных систем и предлагать решения по их совершенствованию	**Неудовлетворительно** не умеет проводить анализ защищенности автоматизированных систем и предлагать решения по их совершенствованию **Удовлетворительно** частично сформированное умение проводить анализ защищенности автоматизированных систем и предлагать решения по их совершенствованию **Хорошо** сформированное, но содержащее пробелы умение проводить анализ защищенности автоматизированных систем и предлагать решения по их совершенствованию **Отлично** Полностью сформированное умение проводить анализ защищенности автоматизированных систем и предлагать решения по их совершенствованию
ПК.3 способность разрабатывать и исследовать модели автоматизированных систем	знать основные программные среды моделирования автоматизированных систем, уметь разрабатывать и исследовать модели автоматизированных систем	**Неудовлетворительно** не знает программные среды моделирования автоматизированных систем, не умеет разрабатывать и исследовать модели автоматизированных систем **Удовлетворительно** частично сформированные знания основных программных сред моделирования автоматизированных систем, частично сформированное умение разрабатывать и исследовать модели автоматизированных систем **Хорошо** сформированные, но содержащие пробелы знания основных программных сред моделирования автоматизированных систем, сформированное, но содержащее пробелы умение разрабатывать и исследовать модели автоматизированных систем **Отлично** Полностью сформированные знания основных программных сред моделирования

		Отлично автоматизированных систем, сформированное умение разрабатывать и исследовать модели автоматизированных систем
ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем	уметь корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий	**Неудовлетворительно** Отсутствие умений корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий **Удовлетворительно** Частично сформированные умения корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий **Хорошо** В целом успешные, но содержащие некоторые пробелы умения корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий **Отлично** Полностью сформированные умения корректировать работу систем защиты информационной системы в зависимости от внешних и внутренних условий
ПСК.1.2 способность разрабатывать и реализовывать политики информационной безопасности открытых информационных систем	Знать нормативную базу, относящуюся к обеспечению информационной безопасности открытых информационных систем, уметь применять ее при формировании политик безопасности предприятия	**Неудовлетворительно** не знает нормативную базу, относящуюся к обеспечению информационной безопасности открытых информационных систем, не умеет применять ее при формировании политик безопасности предприятия **Удовлетворительно** частично сформированные знания нормативной базы, относящейся к обеспечению информационной безопасности открытых информационных систем, частично сформированное умение применять ее при формировании политик безопасности предприятия **Хорошо** сформированные, но содержащие пробелы знания нормативной базы, относящейся к обеспечению информационной безопасности открытых информационных систем, сформированное, но содержащие пробелы умение применять ее при формировании политик безопасности предприятия

		Отлично полностью сформированные знания нормативной базы, относящейся к обеспечению информационной безопасности открытых информационных систем и умение применять ее при формировании политик безопасности предприятия
ПК.8 способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	знать действующие ГОСТы отчетов и публикаций, уметь готовить научно-технические отчеты по результатам выполненных работ, владеть навыками подготовки научно-технической документации	**Неудовлетворительно** не знает действующих ГОСТов для отчетов и публикаций, не умеет готовить научно-технические отчеты по результатам выполненных работ, не владеет навыками подготовки научно-технической документации **Удовлетворительно** частично сформированные знания действующих ГОСТов отчетов и публикаций, частично сформированные умения готовить научно-технические отчеты по результатам выполненных работ, частично сформированные навыки подготовки научно-технической документации **Хорошо** сформированные, но содержащие пробелы знания действующих ГОСТов отчетов и публикаций, сформированные, но содержащие пробелы умения готовить научно-технические отчеты по результатам выполненных работ, сформированные, но содержащие пробелы навыки подготовки научно-технической документации **Отлично** Полностью сформированные знания действующих ГОСТов отчетов и публикаций, сформированные умения готовить научно-технические отчеты по результатам выполненных работ, сформированные навыки подготовки научно-технической документации
ПСК.1.4 способность участвовать в организации и проведении контроля обеспечения информационной безопасности открытой	знать требования обеспечения информационной безопасности открытой информационной системы, уметь контролировать соблюдение мер по ее обеспечению	**Неудовлетворительно** не знает требования обеспечения информационной безопасности открытой информационной системы, не умеет контролировать соблюдение мер по ее обеспечению **Удовлетворительно** частично сформированные знания

информационной системы		**Удовлетворительно** требований обеспечения информационной безопасности открытой информационной системы, частично сформированное умение контролировать соблюдение мер по ее обеспечению информационной безопасности открытой информационной системы **Хорошо** сформированные, но содержащие пробелы знания требований обеспечения информационной безопасности открытой информационной системы, сформированное, но содержащие пробелы умение контролировать соблюдение мер по ее обеспечению информационной безопасности открытой информационной системы **Отлично** полностью сформированные знания требований обеспечения информационной безопасности открытой информационной системы и умение контролировать соблюдение мер по ее обеспечению
ОК.3 способность работать самостоятельно и в коллективе, уметь находить и принимать организационно-управленческие решения, оценивать их эффективность	уметь критически оценивать выполненную работу	**Неудовлетворительно** Отсутствует умение критически оценивать выполненную работу и делать выводы **Удовлетворительно** Частично сформированное умение критически оценивать выполненную работу и делать выводы **Хорошо** Сформированное умение критически оценивать выполненную работу, но наличие ошибок в результатах оценивания **Отлично** Полностью сформированное умение критически оценивать выполненную работу и делать выводы
ПСК.1.3 способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной	знать программные средства проектирования информационных систем, владеть навыками управления информационной безопасностью открытой информационной системы	**Неудовлетворительно** не знает программные средства проектирования информационных систем, не владеет навыками управления информационной безопасностью открытой информационной системы **Удовлетворительно** сформированные, но содержащие пробелы знания программных средств проектирования информационных систем, посредственное владение навыками

системы		**Удовлетворительно** управления информационной безопасностью открытой информационной системы **Хорошо** частично сформированные знания программных средств проектирования информационных систем, неуверенное владение навыками управления информационной безопасностью открытой информационной системы **Отлично** Полностью сформированные знания программных средств проектирования информационных систем, уверенное владение навыками управления информационной безопасностью открытой информационной системы
ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	знать виды угроз для информационной системы, уметь строить модели угроз, вероятности их реализации и определять степень защищенности автоматизированной системы	**Неудовлетворительно** Отсутствуют понятия об угрозах для информационной системы **Удовлетворительно** Присутствуют общие представления об угрозах для информационной системы, частично сформированное умение определять степень защищенности системы и способы построения модели угроз. **Хорошо** Сформированные, но содержащие отдельные пробелы знания в основных понятиях защищенной системы, в видах угроз, их классификации, механизмах защиты. Существуют затруднения в построении модели угроз и определении степени защищенности автоматизированной системы. **Отлично** Полностью сформированное умение построить модель угроз и определить степень защищенности автоматизированной системы
ПСК.1.5 способность формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие	знать комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем и уметь применять их на	**Неудовлетворительно** не знает комплекс мер для обеспечения информационной безопасности открытых информационных систем и не умеет применять их на практике **Удовлетворительно** частично сформированные знания комплекса мер для обеспечения информационной

принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем	практике	**Удовлетворительно** безопасности открытых информационных систем и умение применять их на практике **Хорошо** сформированные, но содержащие пробелы знания комплекса мер для обеспечения информационной безопасности открытых информационных систем и умение применять их на практике **Отлично** Полностью сформированные знания правил, процедур, практических приемов, руководящих принципов, методов и средств для обеспечения информационной безопасности открытых информационных систем и умение применять их на практике

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

Выставляется в случае, если существуют не освоенные компетенции. Студент не выполнил программу производственной практики.	**Неудовлетворительно**
Выставляется в случае усвоения всех компетенций на пороговом уровне. Студент в основном выполнил программу производственной практики и на защите индивидуального отчета показывает достаточные знания специфики математических методов и информационных технологий, применяемых в вузе. Умеет применять теоретические знания для решения некоторых задач по защите информации и реализации мероприятий на практике. Ориентируется в большей части технической документации.	**Удовлетворительно**
Выставляется в случае, если все компетенции освоены. При ответе на вопросы содержались неточности в изложении самостоятельно изученного материала. Студент выполнил программу производственной практики и на защите индивидуального отчета показывает достаточные знания знание комплекса мер по обеспечению информационной безопасности предприятия. Умеет применять теоретические знания на практике. Свободно ориентируется в технической литературе и предоставленной на практике документации.	**Хорошо**
Выставляется в случае, если все компетенции освоены на повышенном уровне по когнитивным и деятельностно-практическим критериям. Студент выполнил всю программу практики и на защите индивидуального отчета	**Отлично**

показывает глубокое и всестороннее знание комплекса мер по обеспечению информационной безопасности предприятия. Свободно ориентируется в литературе и предоставленной на практике документацией.	**Отлично**