ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Директор института
Высшая школа электроники и компьютерных наук

_____Г. И. Радченко
20.07.2017

РАБОЧАЯ ПРОГРАММА
практики
к ОП ВО от 28.06.2017 №007-03-0527

Практика Преддипломная практика
для специальности 10.05.03 Информационная безопасность автоматизированных систем
Уровень специалист **Тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика, к.техн.н., доц. (ученая степень, ученое звание)	_____09.07.2017_____ (подпись)	А. Н. Соколов
Разработчик программы, к.техн.н., доц., заведующий кафедрой (ученая степень, ученое звание, должность)	_____09.07.2017_____ (подпись)	А. Н. Соколов

Челябинск

1. Общая характеристика

Вид практики

Производственная

Способ проведения

Стационарная или выездная

Тип практики

практика по получению профессиональных умений и опыта профессиональной деятельности

Форма проведения

Дискретная

Цель практики

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

Задачи практики

Задачами преддипломной практики являются:
- использование нормативных правовых документов по обеспечению защиты информации;
- изучение принципов формирования комплекса мер по обеспечению информационной безопасности с учетом их правовой обоснованности, административно-управленческой и технической реализуемости, а также экономической целесообразности;
- изучение видов и форм информации, подверженной угрозам, видов и возможных методов и путей реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия;
- участие в эксплуатации и администрировании подсистем управления информационной безопасностью предприятия;
- участие в работах по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;
- проведение предварительного технико-экономического анализа и обоснования

проектных решений по обеспечению информационной безопасности с учетом экономической эффективности разработок;
- оформление рабочей технической документации с учетом действующих нормативных и методических документов в области информационной безопасности;
- применение программных средств системного, прикладного и специального назначения;
- использование инструментальных средств и систем программирования для решения профессиональных задач;
- проведение анализа информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов.

Краткое содержание практики

Преддипломная практика студентов является составной частью основной образовательной программы высшего образования и представляет собой форму организации учебного процесса, непосредственно ориентированную на профессионально-практическую подготовку обучающихся.
Преддипломная практика проводится в сторонних учреждениях, организациях и предприятиях любых организационно-правовых форм (далее организациях), основная деятельность которых предопределяет наличие объектов и видов профессиональной деятельности выпускников по специальности "Информационная безопасность автоматизированных систем" или на кафедрах и в лабораториях вуза, обладающих необходимым кадровым и научно-техническим потенциалом.
Преддипломная практика является завершающим этапом учебного процесса, предназначенным для подготовки выпускной квалификационной работы.

2. Компетенции обучающегося, формируемые в результате прохождения практики

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения при прохождении практики (ЗУНы)
ОК-8 способностью к самоорганизации и самообразованию	Знать:базовые методы и средства самоорганизации и самообразования при подготовке выпускной квалификационной работы.
	Уметь:планировать самостоятельную образовательную деятельность на основе формулирования ближайших и стратегических целей при подготовке выпускной квалификационной работы.
	Владеть:навыками планирования, определения средств и целей самостоятельной деятельности при подготовке выпускной квалификационной работы.
ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Знать:основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения

	информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации.
	Уметь:применять нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации.
	Владеть:навыками работы с нормативными правовыми актами в области обеспечения информационной безопасности и нормативными методическими документами ФСБ России и ФСТЭК России в области защиты информации.
ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Знать:принципы формирования политики информационной безопасности в информационных системах.
	Уметь:определять комплекс мер (правила, процедуры, практические приёмы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем.
	Владеть:методами разработки частных политик информационной безопасности информационных систем.
ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Знать:принципы формирования и анализа проектных решений по обеспечению безопасности автоматизированных систем в соответствии с требованиями по защите информации.
	Уметь:оценивать информационные риски в информационных системах; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.
	Владеть:навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных систем.
ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Знать:свойства, функции и признаки документа, в том числе как объекта нападения и защиты; основы документационного обеспечения

	управления; задачи органов защиты информации на предприятиях; действующие нормативные и методические документы по оформлению рабочей технической документации.
	Уметь:квалифицированно исследовать состав документации предприятия (организации); разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.
	Владеть:методами формирования требований по защите информации.

3. Место практики в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ	Перечень последующих дисциплин, видов работ
Б.1.30.01 Разработка защищенных автоматизированных систем Б.1.38 Комплексное обеспечение защиты информации объекта информатизации Б.1.24.01 Организационное обеспечение информационной безопасности Б.1.23 Криптографические методы защиты информации В.1.10 Обеспечение информационной безопасности на критически важных объектах Б.1.25 Техническая защита информации Б.1.24.02 Правовое обеспечение информационной безопасности Производственная практика (8 семестр)	

Требования к «входным» знаниям, умениям, навыкам студента, необходимым для прохождения данной практики и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.23 Криптографические методы защиты информации	Знать: требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры; принципы построения криптографических алгоритмов. Уметь: эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах. Владеть: криптографической терминологией.

Б.1.30.01 Разработка защищенных автоматизированных систем	Знать: методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем. Уметь: исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений. Владеть: методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем.
Б.1.24.02 Правовое обеспечение информационной безопасности	Знать: основы правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации. Владеть: навыками работы с нормативными правовыми актами.
Б.1.24.01 Организационное обеспечение информационной безопасности	Знать: источники и классификацию угроз информационной безопасности; основы организационного обеспечения информационной безопасности. Уметь: разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов. Владеть: методами формирования требований по защите информации.
Б.1.38 Комплексное обеспечение защиты информации объекта информатизации	Знать: принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации). Уметь: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; выявлять уязвимости информационно-технологических ресурсов информационных систем. Владеть: навыками анализа информационной инфраструктуры информационной системы и ее безопасности; методами выявления угроз информационной безопасности информационных систем.
Б.1.25 Техническая защита информации	Знать: технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам; методы и средства контроля эффективности технической защиты информации. Уметь: анализировать и оценивать угрозы

	информационной безопасности объекта. Владеть: методами и средствами выявления угроз безопасности автоматизированным системам.
В.1.10 Обеспечение информационной безопасности на критически важных объектах	Знать: классы и характеристики критически важных объектов; понятия и определения, на которых базируются решения проблем информационной безопасности критически важных объектов; нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности критически важных объектов. Уметь: реализовывать с учетом особенностей функционирования критически важных объектов требования нормативно-методической и руководящей документации, а также действующего законодательства по вопросам защиты информации ограниченного доступа. Владеть: терминологией и системным подходом при обеспечении информационной безопасности на критически важных объектах.
Производственная практика (8 семестр)	Знать: место информационной безопасности автоматизированных систем в системе национальной безопасности РФ; риски информационной безопасности и проблемы построения комплексной системы защиты информации на предприятии; важность проведения анализа информационной безопасности объектов информатизации и автоматизированных систем. Уметь: выполнять поиск и проводить анализ изменения стандартов в области информационной безопасности. Владеть: навыками проведения анализа защищенности объектов информатизации и автоматизированных систем.

4. Время проведения практики

Время проведения практики (номер уч. недели в соответствии с графиком) с 37 по 40

5. Структура практики

Общая трудоемкость практики составляет зачетных единиц 6, часов 216, недель 4.

№ раздела (этапа)	Наименование разделов (этапов) практики	Кол-во часов	Форма текущего контроля
1	Организационный	8	Проверка дневника прохождения практики
2	Основной	144	Проверка дневника

			прохождения практики
3	Итоговый	64	Проверка отчета о прохождении практики

6. Содержание практики

№ раздела (этапа)	Наименование или краткое содержание вида работ на практике	Кол-во часов
1	Введение. Постановка задач практики. Производственный инструктаж, в том числе инструктаж по технике безопасности.	8
2.1	Знакомство с организацией и анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности: - автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите; - информационных технологий, формирующих информационную инфраструктуру предприятия (организации) в условиях существования угроз в информационной сфере и задействующих информационно-технологические ресурсы, подлежащие защите; - технологий обеспечения информационной безопасности автоматизированных систем; - систем управления информационной безопасностью автоматизированных систем. Выбор объекта проектирования. Сбор, обработка и систематизация фактического материала по выбранному объекту проектирования.	24
2.2	Знакомство с нормативными правовыми актами в области обеспечения информационной безопасности и нормативными методическими документами ФСБ России и ФСТЭК России в области защиты информации, необходимыми для обеспечения информационной безопасности выбранного объекта проектирования.	24
2.3	Разработка комплекса организационно-технических мероприятий, необходимых для обеспечения информационной безопасности выбранного объекта проектирования.	24
2.4	Выбор программно-аппаратных и технических средств защиты информации, необходимых для обеспечения информационной безопасности выбранного объекта проектирования.	24
2.5	Разработка документационного обеспечения защиты информации выбранного объекта проектирования.	24
2.6	Проведение технико-экономического обоснования разработанных проектных решений для обеспечения защиты информации выбранного объекта проектирования. Вопросы ТБ, ОТ и БЖД.	24
3	Оформление отчета по преддипломной практике.	64

7. Формы отчетности по практике

По окончанию практики, студент предоставляет на кафедру пакет документов, который включает в себя:
- дневник прохождения практики, включая индивидуальное задание и характеристику работы практиканта организацией;
- отчет о прохождении практики.
Формы документов утверждены распоряжением заведующего кафедрой от 31.08.2016 №308-03-04.

8. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

Форма итогового контроля – оценка.

8.1. Паспорт фонда оценочных средств

Наименование разделов практики	Код контролируемой компетенции (или ее части)	Вид контроля
Организационный	ОК-8 способностью к самоорганизации и самообразованию	Проверка дневника прохождения практики
Основной	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Проверка дневника прохождения практики
Основной	ПК-27 способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	Проверка дневника прохождения практики
Основной	ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Проверка дневника прохождения практики
Итоговый	ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Проверка дневника прохождения практики
Все разделы	ОК-8 способностью к самоорганизации и самообразованию	Дифференцированный зачет
Все разделы	ОПК-6 способностью применять нормативные правовые акты в профессиональной деятельности	Дифференцированный зачет
Все разделы	ПК-27 способностью выполнять	Дифференцированный

	полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	зачет
Все разделы	ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	Дифференцированный зачет
Все разделы	ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем	Дифференцированный зачет

8.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Проверка дневника прохождения практики	В процессе прохождения практики проверяется корректность и полнота заполнения соответствующих разделов дневника.	Зачтено: Дневник прохождения практики корректно заполнен и отражает все разделы практики, приведенные в данной программе. Не зачтено: Дневник прохождения практики заполнен не корректно и/или не отражает какие-либо разделы практики, приведенные в данной программе.
Дифференцированный зачет	К зачету допускаются студенты, представившие заверенные по месту проведения практики Дневник прохождения практики (включающий индивидуальное задание и характеристику работы практиканта организацией) и Отчет о прохождении практики. Зачет проводится в устной форме в виде защиты представленного	Отлично: выставляется за полностью раскрытые вопросы на высоком качественном уровне. Хорошо: выставляется в том случае, если вопросы раскрыты хорошо с достаточной степенью полноты и содержательности. Удовлетворительно: выставляется в том случае,

	Отчета о прохождении практики, в ходе которого студент отвечает на поставленные вопросы об особенностях прохождения практики.	если вопросы раскрыты удовлетворительно, но имеются замечания по полноте и содержанию ответа. Неудовлетворительно: выставляется, если содержание ответов не совпадает с поставленными вопросами или ответ отсутствует.

8.3. Примерный перечень индивидуальных заданий

1. Организация безопасного удаленного доступа к ЛВС предприятия (название предприятия).
2. Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии (название предприятия).
3. Автоматизация учета конфиденциальных документов на предприятии (название предприятия).
4. Организация процессов мониторинга конфиденциального документооборота на предприятии (название предприятия).
5. Автоматизация процесса проверок наличия конфиденциальных документов на предприятии (название предприятия).
6. Разработка комплексной системы защиты информации (КСЗИ) предпри-ятия (название предприятия).
7. Организация системы планирования и контроля функционирования КСЗИ на предприятии (название предприятия).
8. Разработка основных направлений совершенствования КСЗИ предприятия (наименование предприятия).
9. Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии (наименование предприятия).
10. Разработка методологии проектирования КСЗИ.
11. Разработка моделей процессов защиты информации при проектировании КСЗИ.
12. Анализ методов оценки качества функционирования КСЗИ.
13. Разработка структурно-функциональной модели управления КСЗИ предприятия (наименование предприятия).
14. Разработка проекта программно-аппаратной защиты информации предприятия (наименование предприятия).
15. Разработка методов расчета экономической эффективности программно-аппаратной защиты информации предприятия (наименование предприятия).
16. Криптографические средства защиты информации на основе дискретных носителей.
17. Разработка игровой (дискретной) модели программно-аппаратной защиты информации предприятия (наименование предприятия).
18. Разработка изолированной программно-аппаратной среды в Windows NT (WINDOWS 2000, LINUX и т.д.) (наименование предприятия).

19. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии (название предприятия).
20. Анализ нормативно-правовой базы по защите информации в сети Интернет. Разработка требований по организационной защите конфиденциальной информации, передаваемой и получаемой по сети Интернет (название предприятия).
21. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями (название предприятия).
22. Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации (название предприятия).
23. Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами (название предприятия).
24. Организация порядка установления внутриобъектного спецрежима на объекте информатизации (название предприятия).
25. Использование институтов правовой защиты интеллектуальной собственности для защиты информации (название объекта).
26. Организация защиты персональных данных на основе использования правовых мер (название предприятия).
27. Разработка комплексной системы защиты информации на предприятии, осуществляющем изготовление роботов, оснащенных программным обеспечением, представляющем коммерческую тайну (название предприятия).
28. Разработка и анализ эффективности внедрения мер по защите информации торговых автоматов, подключенных к глобальной сети и управляемых удаленно (название предприятия).
29. Разработка организационно-технических мероприятий по обеспечению безопасности функционирующей информационно-вычислительной системы при вводе в эксплуатацию (внедрении) ее дополнительных очередей (подсистем) сторонними организациями (название предприятия).
30. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия).
31. Комплексная система организация безопасного удаленного доступа к ЛВС предприятия (название предприятия).
32. Комплексная автоматизированная система учета конфиденциальных документов на предприятии (название предприятия).
33. Разработка комплексной системы защиты информации (КСЗИ) предприятия (название предприятия).
34. Организация комплексной системы планирования и контроля функционирования КСЗИ на предприятии (название предприятия).
35. Разработка основных направлений совершенствования КСЗИ предприятия (наименование предприятия).
36. Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии (наименование предприятия).
37. Разработка методологии проектирования КСЗИ.
38. Разработка моделей процессов защиты информации при проектировании КСЗИ.
39. Анализ методов оценки качества функционирования КСЗИ.
40. Разработка структурно-функциональной модели управления КСЗИ предприятия

(наименование предприятия).
41. Разработка проекта комплексной системы программно-аппаратной защиты информации предприятия (наименование предприятия).
42. Разработка методов расчета экономической эффективности комплексной системы защиты информации предприятия (наименование предприятия).
43. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии (название предприятия).
44. Анализ нормативно-правовой базы по комплексной системы защиты информации в сети Интернет. Разработка требований по организационной защите конфиденциальной информации, передаваемой и получаемой по сети Интернет (название предприятия).
45. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями (название предприятия).
46. Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации (название предприятия).
47. Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами (название предприятия).
48. Организация порядка установления внутриобъектного спецрежима на объекте информатизации (название предприятия).
49. Использование институтов правовой защиты интеллектуальной собственности для защиты информации (название объекта).
50. Организация защиты персональных данных на основе использования правовых мер (название предприятия).
51. Разработка комплексной системы защиты информации на предприятии, осуществляющем изготовление роботов, оснащенных программным обеспечением, представляющем коммерческую тайну (название предприятия).
52. Разработка и анализ эффективности внедрения мер по защите информации торговых автоматов, подключенных к глобальной сети и управляемых удаленно (название предприятия).
53. Разработка организационно-технических мероприятий по обеспечению безопасности функционирующей информационно-вычислительной системы при вводе в эксплуатацию (внедрении) ее дополнительных очередей (подсистем) сторонними организациями (название предприятия).
54. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия).
55. Разработка комплексных систем видеонаблюдения и сигнализации для обеспечения защиты информации в (название предприятия).
56. Организация автоматизированного пропускного режима на крупном предприятии (на примере).
57. Разработка комплексной системы защиты информации в кабинете директора (название предприятия).
58. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии .
59. Разработка системы защиты информации конфиденциального характера от утечки по техническим каналам в (название предприятия).

60. Разработка организационного порядка установления внутриобъектного режима для торговой фирмы (название предприятия).
61. Автоматизация обеспечения информационной безопасности группы компаний на базе ОС Unix/Linux.
62. Построение алгоритма системы идентификации, защищенной от подделки продукции.
63. Организация системы контроля доступа и защиты информации на предприятии (на примере ООО «Передвижная механизированная колонна-4»).
64. Разработка комплексной системы защиты информации в кабинете руководителя предприятия.
65. Защита речевой информации в каналах связи коммерческих организаций.
66. Разработка проекта корпоративной сети (название предприятия).
67. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада (название предприятия).
68. Разработка мероприятий организационного характера по обеспечению комплексной защиты информации для (название предприятия).
69. Разработка систем видеонаблюдения и контроля доступа к объектам информатизации в (название предприятия).
70. Анализ методов и форм работы с персоналом, допущенным к конфиденциальной информации, и разработка рекомендаций по их применению для торговых организаций.
71. «Исследование принципов построения биометрических систем контроля доступа на основе анализа рукописного почерка».
72. «Исследование характеристик систем стеганографии звуковых данных с использованием дискретного вейвлет-преобразования».
73. «Корреляционный анализ предупреждений системы обнаружения атак на основе нечеткой логики».
74. «Разработка методов и алгоритмов защиты исходного кода программ от несанкционированного доступа».
75. «Разработка методики оценки эффективности средств зашиты информа-ции».
76. «Система защиты данных в корпоративных сетях на основе криптографических методов».
77. «Система обнаружения атак на основе искусственной нейронной сети».
78. «Система контроля движения на охраняемом объекте с помощью активных радиоволновых технических средств».
79. «Программа внедрения цифровых водяных знаков в звуковые данные с использованием эхоэффекта».
80. «Разработка комплексной системы защиты информации (название предприятия)».
81. «Повышение информационной безопасности корпоративной вычисли-тельной сети (название предприятия)».

9. Учебно-методическое и информационное обеспечение практики

Печатная учебно-методическая документация

а) основная литература:

1. Северин, В. А Комплексная защита информации на предприятии [Текст] учебник для вузов по направлению "Юриспруденция" и специальности "Юриспруденция" В. А. Северин ; под ред. Б. И. Пугинского. - М.: Городец, 2008. - 366 с.
2. Хорев, П. Б. Программно-аппаратная защита информации [Текст] учеб. пособие для вузов по направлению 10.03.01 "Информ. безопасность" П. Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум : ИНФРА-М, 2017. - 351 с. ил.
3. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях [Текст] В. Ф. Шаньгин. - М.: ДМК ПРЕСС, 2012. - 592 с. ил.

б) дополнительная литература:

1. ГОСТ Р 50922-2006 : Защита информации. Основные термины и определения : утв. и введ. в действие 27.12.06 : взамен ГОСТ Р 50922-96 [Текст] Федер. агентство по техн. регулированию и метрологии. - М.: Стандартинформ, 2008. - 7 с.
2. ГОСТ Р 51275-2006 : Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения : утв. и введ. в действие от 27.12.06 : взамен ГОСТ Р 51275-99 [Текст] Федер. агентство по техн. регулированию и метрологии. - М.: Стандартинформ, 2007. - 7 с.
3. ГОСТ Р 52069.0-2003 : Защита информации. Система стандартов. Основные положения : введ. в действие с 01.01.04 [Текст] Гос. науч.-исслед. испытат. ин-т проблем техн. защиты информ. Гос. техн. комиссии при Президенте Рос Федерации и др. - М.: Госстандарт России, 2003. - 11 с.
4. ГОСТ Р 52447-2005: Защита информации. Техника защиты информации. Номенклатура показателей качества : утв. и введ. в действие 29.12.05 [Текст] Федер. агентство по техн. регулированию и метрологии. - М.: Стандартинформ, 2006. - 23 с. ил.
5. ГОСТ Р 53114-2008 : Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения : утв. и введ. в действие от 18.12.08 [Текст] Федер. агентство по техн. регулированию и метрологии. - М.: Стандартинформ, 2009. - 15 с.

из них методические указания для самостоятельной работы студента:

1. Форма дневника прохождения практики
2. Форма отчета о прохождении практики

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Дополнительная литература	Киселева, Э.М. Методические рекомендации по организации и проведению производственной практики студентов бакалавриата. [Электронный	Электронно-библиотечная система Издательства	Интернет / Авторизованный

		ресурс] / Э.М. Киселева, Г.А. Костецкая, Р.И. Попова. — Электрон. дан. — СПб. : РГПУ им. А. И. Герцена, 2014. — 56 с.	Лань	
2	Основная литература	Шаньгин, В.Ф. Защита компьютерной информации. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2010. — 544 с.	Электронно-библиотечная система Издательства Лань	Интернет / Авторизованный

10. Информационные технологии, используемые при проведении практики

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)
2. Microsoft-Windows(бессрочно)

Перечень используемых информационных справочных систем:

1. -Стандартинформ(бессрочно)
2. -Консультант Плюс(31.07.2017)
3. -Гарант(31.12.2017)

11. Материально-техническое обеспечение практики

Место прохождения практики	Адрес места прохождения	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, обеспечивающие прохождение практики
ФГУП "Приборостроительный завод", г.Трехгорный	456080, г. Трехгорный, ул. Заречная, 13	Стенды для отладки и испытаний микроэлектронного оборудования, серверы, ЛВС
ООО "Стратегия безопасности"	454052, г.Челябинск, ул. Пети Калмыкова, д.11-А	Программно-аппаратные комплексы по защите информации и оценке защищенности объектов информатизации.
АО "Челябинский радиозавод "Полет"	454080, Челябинск, ул. Тернопольская, 6	Стенды для отладки и испытаний микроэлектронного оборудования, серверы, ЛВС, средства доступа к глобальной сети