МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики
М.О. Таныгин
(подпись, инициалы, фамилия)
«30» 04 2021 г

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Производственная практика
(наименование вида практики)

Эксплуатационная практика
(наименование типа практики)

направление подготовки (специальность) *10.03.01*
(шифр согласно ФГОС
Информационная безопасность
и наименование направление подготовки (специальности)

Безопасность автоматизированных систем
наименование профиля, специализации или магистерской программы

форма обучения *очная*
(очная, очно-заочная, заочная)

Курск – 2021

6

Программа составлена в соответствии с:

- федеральным государственным образовательным стандартом высшего образования по направлению подготовки *10.03.01 – «Информационная безопасность»*, утвержденным приказом Министерства образования и науки РФ от 01.12.2016 г. №1515 и на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, направленность «Безопасность автоматизированных систем», одобренным Ученым советом университета (протокол №5 «30» января 2017 г.).

Программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки *10.03.01 – «Информационная безопасность»* на заседании кафедры информационной безопасности.
«28» августа 2017г. Протокол № 1

И.о. зав. кафедрой ИБ — Таныгин М.О.

Разработчик программы
доцент кафедры ИБ, к.т.н. — Калуцкий И.В.

Директор научной библиотеки — Макаровская В.Г.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Учены советом университета протокол №5 «30» января 2017 г. на заседании кафедры информационной безопасности, протокол №12 от 29.06.18

Зав. кафедрой _____ Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №5 «30» января 2017 г. на заседании кафедры информационной безопасности, протокол №11 от 27.06.2019

Зав. кафедрой _____ Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №5 «30» января 2017 г. на заседании кафедры информационной безопасности протокол №1 от 31.08.2020

Зав. кафедрой _____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 «Информационная безопасность», одобренного Ученым советом университета протокол №9 «24» 03 2021 г. на заседании кафедры информационной безопасности, №1 от 30.08.2021
(наименование кафедры, дата, номер протокола)

Зав. кафедрой
_____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 «Информационная безопасность», одобренного Ученым советом университета протокол №7 «25» 02 2022 г. на заседании кафедры информационной безопасности протокол №11 от 30.06.2022
(наименование кафедры, дата, номер протокола)

Зав. кафедрой
_____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 «Информационная безопасность», одобренного Ученым советом университета протокол №_ «__»_____20_ г. на заседании кафедры _____
(наименование кафедры, дата, номер протокола)

Зав. кафедрой
_____

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 «Информационная безопасность», одобренного Ученым советом университета протокол №_ «__»_____20_ г. на заседании кафедры _____
(наименование кафедры, дата, номер протокола)

Зав. кафедрой
_____

1 Цель и задачи практики. Вид, тип, способ и форма (-ы) ее проведения

1.1. Цель практики

Целью производственной (эксплуатационной) практики является закрепление теоретических знаний, полученных при изучении базовых дисциплин и приобретение практических навыков будущей профессиональной деятельности в соответствии с выбранной специализацией *10.03.01 – «Информационная безопасность»*.

1.2. Задачи практики

1. Формирование общекультурных и профессиональных компетенций, установленных ФГОС ВО и закрепленных учебным планом за производственной практикой по получению профессиональных умений и профессионального опыта.
2. Освоение современных информационных технологий и профессиональных программных комплексов, применяемых в области информационной безопасности.
3. Совершенствование навыков подготовки, представления и защиты информационных, аналитических и отчетных документов по результатам профессиональной деятельности и практики.
4. Развитие исполнительских и лидерских навыков обучающихся.

1.3 Вид, тип, способ и форма (-ы) ее проведения

Вид практики – производственная.

Тип практики – эксплуатационная.

Способ проведения практики – стационарная (в г. Курске) и выездная (за пределами г. Курска). ФГОС ВО разрешает оба способа проведения данной практики, поэтому способ ее проведения устанавливается конкретно для каждого обучающего в зависимости от места расположения предприятия, организации, учреждения, в котором он проходит практику.

Практика проводится на предприятиях, в организациях и учреждениях, с которыми университетом заключены соответствующие договоры.

Практика проводится на предприятиях различных отраслей и форм собственности, в органах государственной или муниципальной власти, академических или ведомственных научно-исследовательских организациях, учреждениях системы высшего или дополнительного профессионального образования, деятельность которых связана с вопросами информационной безопасности и соответствует профессиональным компетенциям, осваиваемым в рамках образовательной программы: в ФОИВ РФ, ФОИВ субъектов РФ и муниципальных образований, на кафедрах информационной безопасности, обладающих необходимым кадровым и научно-техническим потенциалом, и т.п.

Обучающиеся, совмещающие обучение с трудовой деятельностью, вправе проходить практику по месту трудовой деятельности в случаях, если профессиональная деятельность, осуществляемая ими, соответствует требованиям к содержанию практики, представленному в разделе 4 настоящей программы.

Выбор мест прохождения практики для лиц с ограниченными возможностями здоровья производится с учетом состояния здоровья обучающихся и требований по доступности.

*Форма проведения практики** Производственная (эксплуатационная) практика проходит непрерывно в 8 семестре на 4 курсе, продолжительность - 4 недели.

2 Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (компетенции)		*Планируемые результаты обучения при прохождении практики (компоненты компетенций: знания, умения и навыки)*
Код компетенции	*Содержание компетенции*	
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	***Знать:*** основные особенности эксплуатации программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.
		Уметь: самостоятельно выполнять работы по установке и обслуживанию различных средств защиты информации.
		Владеть: навыками формирования требований по обеспечению надежности аппаратных средств вычислительной техники. методами и средствами выявления неисправностей автоматизированных систем. осуществлять поиск наиболее эффективных путей обработки информации и (или) ее управления.
ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	***Знать:*** принципы работы программных, программно-аппаратных криптографических средств и технических средств зашиты информации; принципы работы программных средств системного, прикладного и специального назначения, знать языки и системы программирования для решения профессиональных задач по криптографической защите информации.
		Уметь: применять полученные знания при решении разного рода задач по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; разрабатывать алгоритмы применения криптографических программных средств системного, прикладного и специального назначения.
		Владеть: навыками работы с программными средствами системного, прикладного и специального назначения, инструментальными средствами, языками и системами программирования для решения задач по по-

Планируемые результаты освоения образовательной программы (компетенции)		*Планируемые результаты обучения при прохождении практики (компоненты компетенций: знания, умения и навыки)*
Код компетенции	*Содержание компетенции*	
		строению систем информационной безопасности.
ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты	***Знать:*** основные принципы администрирования подсистемы информационной безопасности.
		Уметь: устанавливать, настраивать, эксплуатировать и поддерживать в работоспособном состоянии компоненты системы обеспечения информационной безопасности с учетом установленных требований.
		Владеть: навыками работы в СЗИ VipNet, SecretNet
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	***Знать:*** основную правовую законодательную базу в области информационной безопасности, типовые политики информационной безопасности объектов.
		Уметь: осуществлять комплексное организационно-правовое обеспечение информационной безопасности объекта защиты, разрабатывать соответствующие политики безопасности на объекте.
		Владеть: навыками изучения и обобщения опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государственной и других видов тайны.
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	***Знать:*** законы, технологии, правила аттестации объекта информатизации.
		Уметь: проводить аттестацию объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации.
		Владеть: уавыками разработки технологической и эксплуатационной документации.
ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	***Знать:*** - номенклатуру современных программно-аппаратных и технических средств защиты информации; - назначение, организацию и принципы функционировании программно-аппаратных средств защиты информации; - механизмы защиты объектов, реализованные программно-аппаратных средств защиты информации; - способы, методы и технические средства защиты

Планируемые результаты освоения образовательной программы (компетенции)		*Планируемые результаты обучения при прохождении практики (компоненты компетенций: знания, умения и навыки)*
Код компетенции	*Содержание компетенции*	
		конфиденциальной информации - основные положения РД по защите информации на объектах защиты.
		Уметь: - сопоставлять структурную и функциональную организацию программных и аппаратных средств защиты информации требованиям политики безопасности; - анализировать механизмы реализации методов защиты конкретных объектов и процессов для решения профессиональных задач; - выявлять уязвимости в эксплуатируемых технических средствах защиты информации.
		Владеть: - навыками реализации требуемых политик безопасности с помощью современных программно-аппаратных средств защиты информации; - проведения проверок работоспособности и эффективности применения программно-аппаратных и технических средств защиты информации.
ПСК-4.2	способность выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	***Знать:*** - принципы построения современных операционных систем; - особенности организации средств защиты в распределенных СУБД; - назначение, организацию и принципы функционировании файловых систем; - механизмы защиты информационно-вычислительных сетей, реализованных средствами операционных систем и дополнительного программного обеспечения.
		Уметь: - администрировать подсистемы управления доступа современных операционных систем и программно-аппаратные средства защиты информации; - пользоваться средствами защиты, предоставляемыми СУБД; - устанавливать и настраивать операционные системы и их подсистемы обеспечения информационной безопасности.
		Владеть: - навыками работы администратора по защите в базе данных; - навыками реализации требуемых политик безопасности средствами операционных систем; - навыками оценки эффективности работы операционной системы и её подсистем обеспечения инфор-

Планируемые результаты освоения образовательной программы (компетенции)		*Планируемые результаты обучения при прохождении практики (компоненты компетенций: знания, умения и навыки)*
Код компетенции	*Содержание компетенции*	
		мационной безопасности; - навыками администрирования клиентских операционных систем; - навыками использования комплексов управления информационной безопасностью с учетом особенностей объектов защиты; восстановления данных

3 Место практики в структуре образовательной программы. Объем практики в зачетных единицах и ее продолжительности в неделях либо в академических или астрономических часах

В соответствии с учебным планом производственная эксплуатационная практика (Б2.П.2) входит в блок Б2 «Практики, в том числе научно-исследовательская работа».

Практика является обязательным разделом образовательной программы и представляет собой вид учебных занятий, направленный на формирование, закрепление, развитие практических умений, навыков и компетенций в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью. Практика тесно связана с ранее изученными дисциплинами и направлена на обеспечение непрерывности и последовательности овладения обучающимися видами профессиональной деятельности, установленными образовательной программой.

Эксплуатационная практика проводится на 4-м курсе в 8-м семестре.

Объем производственной эксплуатационной практики, установленный учебным планом, – 4 зачетных единиц, продолжительность – 2,2/3 недели (144 часов).

4 Содержание практики

Содержание практики уточняется для каждого обучающегося в зависимости от специфики конкретного предприятия, организации, учреждения, являющегося местом ее проведения, и выдается в форме задания на практику.

Таблица 4 – Этапы и содержание практики

№ п/п	Этапы практики	Содержание практики	Трудоемкость (час)
1	Подготовительный этап	Решение организационных вопросов: 1) распределение обучающихся по местам практики; 2) знакомство с целью, задачами, программой, порядком прохождения практики; 3) получение заданий от руководителя	2

		практики от университета; 4) информация о требованиях к отчетным документам по практике; 5) первичный инструктаж по технике безопасности.	
2	Подготовительный этап (работа на предприятии)	Решение организационных вопросов на предприятии: 1) Знакомство с предприятием, с внутренним распорядком предприятия, руководителем практики от предприятия, рабочим местом и должностной инструкцией. 2) Проведение инструктажей по технике безопасности на рабочем месте, противопожарной профилактике. 3) получение задания от руководителя практики от предприятия.	10
3	Основной этап (работа на предприятии)	Изучение нормативных документов, регулирующих работу, относящуюся к должностным обязанностям (положения, приказы, инструкции, памятки и др)	96
		Выполнение индивидуального задания на практику	
3	Заключительный этап	Оформление дневника практики.	36
		Составление отчета о практике.	
		Представление дневника практики и защита отчета о практике на промежуточной аттестации.	

Эксплуатационная практика должна включать в себя в обязательном порядке следующие мероприятия:

- получение теоретических знаний;
- практическую работу.

Для прохождения практики каждому студенту выдается индивидуальное задание.

Индивидуальное задание включает техническое задание, которое выполняется студентами самостоятельно.

5 Формы отчетности по практике

Формы отчетности студентов о прохождении производственной эксплуатационной практики:

- дневник практики
(https://www.swsu.ru/structura/umu/training_division/blanks.php),
- отчет о практике.

Структура отчета о эксплуатационной практике:

1) Титульный лист.
2) Содержание.
3) Введение. Цель и задачи практики. Общие сведения о предприятии, организации, учреждении, на котором проходила практика.
4) Основная часть отчета.
5) Заключение. Выводы о достижении цели и выполнении задач практики.
6) Список использованной литературы и источников.
7) Приложения (иллюстрации, таблицы, карты и т.п.).

Отчет должен быть оформлен в соответствии с:

- ГОСТ Р 7.0.12-2011 Библиографическая запись. Сокращение слов и словосочетаний на русском языке. Общие требования и правила.
- ГОСТ 2.316-2008 Единая система конструкторской документации. Правила нанесения надписей, технических требований и таблиц на графических документах. Общие положения;
- ГОСТ 7.32-2001 Отчет о научно-исследовательской работе. Структура и правила оформления;
- ГОСТ 2.105-95 ЕСКД. Общие требования к текстовым документам;
- ГОСТ 7.1-2003 Система стандартов по информации, библиотечному и издательскому делу. Общие требования и правила составления;
- ГОСТ 2.301-68 Единая система конструкторской документации. Форматы;
- ГОСТ 7.82-2001 Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления;
- ГОСТ 7.9-95 (ИСО 214-76). Система стандартов по информации, библиотечному и издательскому делу. Реферат и аннотация. Общие требования.
-СТУ 04.02.030-2015 «Курсовые работы (проекты). Выпускные квалификационные работы. Общие требования к структуре и оформлению»

6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), практики, НИР, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ПК-1 - способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Аппаратные средства вычислительной техники Криптографические методы защиты информации Безопасность сетей ЭВМ Введение в криптографию Ознакомительная практика Технологическая практика	Программно-аппаратные средства защиты информации Инженерно-техническая защита информации Эксплуатационная практика	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
ПК-2 - способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Криптографические методы защиты информации Языки программирования Технологии и методы программирования Информационные технологии Введение в криптографию Основы ривер-синжениринга программных средств Методы защиты программного обеспечения Ознакомительная практика	Эксплуатационная практика	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
ПК-3 - способность администрировать подсистемы информационной безопасности объекта защи-	Информационные технологии Безопасность операционных систем Технические средства охраны Системы контроля	Техническая защита информации Эксплуатационная практика	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), практики, НИР, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ты	доступа и видеонаблюдения		
ПК-4 - способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Управление информационной безопасностью Введение в направление подготовки и планирование профессиональной карьеры	Защита информационных процессов в компьютерных системах Защита и обработка конфиденциальных документов Сети и системы передачи информации (специальные разделы) Беспроводные сети связи Эксплуатационная практика	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
ПК-5 - способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Технологическая практика	Техническая защита информации Инженерно-техническая защита информации Эксплуатационная практика	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
ПК-6 - способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Основы реверсинжиниринга программных средств Методы защиты программного обеспечения	Программно-аппаратные средства защиты информации Техническая защита информации Защита информационных процессов в компьютерных системах Эксплуатационная практика	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты
ПСК-4.2 - способность выполнять комплекс задач администрирования	Безопасность систем баз данных Безопасность операционных систем	Администрирование вычислительных сетей Сети и системы передачи информа-	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), практики, НИР, при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей		ции (специальные разделы) Беспроводные сети связи Эксплуатационная практика	

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции/ этап *(указывается название этапа из п.6.1)*	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
ПК-1/ завершающий	*1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.2. программы практики* *2.Качество освоенных обучающимся знаний, умений, навыков* *3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях.*	**Знает:** Элементарные принципы эксплуатации программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. **Умеет:** В недостаточной мере выполнять работы по установке и обслуживанию различных средств защиты информации. **Владеет:** Элементарными навыками формирования требований по обеспечению надежности аппаратных средств вы-	**Знает:** Сформированные принципы эксплуатации программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. **Умеет:** Сформированное умение самостоятельно выполнять работы по установке и обслуживанию различных средств защиты информации **Владеет:** Основными навыками формирования требований по обеспечению надежности аппаратных	**Знает:** Глубокие знания эксплуатации программ-ных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации. **Умеет:** Сформированное в полной мере умение самостоятельно выполнять работы по установке и обслуживанию различных средств защиты информации **Владеет:** Уверенными навыками формирования требований по обеспечению надежно-

Код компетенции/ этап *(указывается название этапа из п.6.1)*	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
		числительной техники; методами и средствами выявления неисправностей автоматизированных систем; осуществлять поиск наиболее эффективных путей обработки информации и (или) ее управления.	средств вычислительной техники; методами и средствами выявления неисправностей автоматизированных систем; осуществлять поиск наиболее эффективных путей обработки информации и (или) ее управления.	сти аппаратных средств вычислительной техники; методами и средствами выявления неисправностей автоматизированных систем; осуществлять поиск наиболее эффективных путей обработки информации и (или) ее управления.
ПК-2/ завершающий	*1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.2. программы практики* *2.Качество освоенных обучающимся знаний, умений, навыков* *3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	**Знает**: поверхностно принципы работы программных, программно-аппаратных криптографических средств и технических средств зашиты информации; принципы работы программных средств системного, прикладного и специального назначения, знать языки и системы программирования для решения профессиональных задач по криптографической защите информации. **Умеет**: в недостаточной мере применять полученные знания при решении разного рода задач по установке, настройке и обслуживанию программных, программно-аппаратных (в том	**Знает**: Углубленно, но с некоторыми пробелами в отдельных областях, принципы работы программных, программно-аппаратных криптографических средств и технических средств зашиты информации; принципы работы программных средств системного, прикладного и специального назначения, знать языки и системы программирования для решения профессиональных задач по криптографической защите информации. **Умеет**: в достаточной мере применять полученные знания при решении разного рода задач по установке, настройке и обслуживанию	**Знает**: Углубленно принципы работы программных, программно-аппаратных криптографических средств и технических средств зашиты информации; принципы работы программных средств системного, прикладного и специального назначения, знать языки и системы программирования для решения профессиональных задач по криптографической защите информации. **Умеет**: успешно применять полученные знания при решении разного рода задач по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографи-

Код компетенции/ этап *(указывается название этапа из п.6.1)*	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
		числе криптографических) и технических средств защиты информации; разрабатывать алгоритмы применения криптографических программных средств системного, прикладного и специального назначения. **Владеет:** слабо владеет навыками работы с программными средствами системного, прикладного и специального назначения, инструментальными средствами, языками и системами программирования для решения задач по построению систем информационной безопасности. .	программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; разрабатывать алгоритмы применения криптографических программных средств системного, прикладного и специального назначения. **Владеет**: навыками работы с программными средствами системного, прикладного и специального назначения, инструментальными средствами, языками и системами программирования для решения задач по построению систем информационной безопасности.	ческих) и технических средств защиты информации; разрабатывать алгоритмы применения криптографических программных средств системного, прикладного и специального назначения. **Владеет**: развитыми навыками работы с программными средствами системного, прикладного и специального назначения, инструментальными средствами, языками и системами программирования для решения задач по построению систем информационной безопасности.
ПК-3/ завершающий	*1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.2. программы практики* *2.Качество освоенных обучающимся знаний, умений, навыков*	**Знает:** Поверхностные знания основных принципов администрирования подсистемы информационной безопасности. **Умеет:** Испытывает затруднения при установке, настройке, эксплуатации и поддержке в работоспособном состоянии компонентов системы обеспечения ин-	**Знает:** Сформированные, но содержащие отдельные пробелы знания основных принципов администрирования подсистемы информационной безопасности. **Умеет:** Способен устанавливать, настраивать, эксплуатировать и поддерживать в работоспособном состоянии компоненты	**Знает:** Глубокие знания основных принципов администрирования подсистемы информационной безопасности. **Умеет:** Способен самостоятельно устанавливать, настраивать, эксплуатировать и поддерживать в работоспособном состоянии компоненты

Код компетенции/ этап *(указывается название этапа из п.6.1)*	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях.	формационной безопасности с учетом установленных требований. **Владеет:** элементарными навыками работы в СЗИ VipNet, SecretNet.	системы обеспечения информационной безопасности с учетом установленных требований. **Владеет:** основными навыками работы в СЗИ VipNet, SecretNet.	системы обеспечения информационной безопасности с учетом установленных требований. **Владеет:** Уверенно владеет навыками работы в СЗИ VipNet, SecretNet.
ПК-4/ завершающий	*1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.2. программы практики* *2.Качество освоенных обучающимся знаний, умений, навыков* *3.Умение применять знания, умения, навыки в типовых и нестандартных ситуациях*	**Знает:** Поверхностные знания основной правовую законодательной базы в области информационной безопасности, типовых политик информационной безопасности объектов. **Умеет:** Испытывает затруднения при осуществлении комплексного организационно-правового обеспечения информационной безопасности объекта защиты, разработке соответствующих политик безопасности на объекте **Владеет:** элементарными навыками изучения и обобщения опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохра-	**Знает:** Сформированные знания основной правовую законодательной базы в области информационной безопасности, типовых политик информационной безопасности объектов. **Умеет:** Способен осуществлять комплексное организационно-правовое обеспечение информационной безопасности объекта защиты, разрабатывать соответствующие политики безопасности на объекте. **Владеет:** Основными навыками изучения и обобщения опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохра-	**Знает:** Глубокие знания основной правовую законодательной базы в области информационной безопасности, типовых политик информационной безопасности объектов. **Умеет:** Способен уверенно осуществлять комплексное организационно-правовое обеспечение информационной безопасности объекта защиты, разрабатывать соответствующие политики безопасности на объекте. **Владеет:** Уверенными навыками изучения и обобщения опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации и сохранения государствен-

Код компетенции/ этап *(указывается название этапа из п.6.1)*	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
		нения государственной и других видов тайны.	нения государственной и других видов тайны.	ной и других видов тайны.
ПК-5/ завершающий	*1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.2. программы практики* *2.Качество освоенных обучающимся знаний, умений, навыков* *3.Умение применять знания, умения, навыки в типовых и нестандартных ситуаци-ях*	**Знать:** Поверхностные знания законов, технологии, правил аттестации объекта информатизации. **Уметь:** Испытывает затруднения при проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации. **Владеть:** Элементарными навыками разработки технологической и эксплуатационной документации.	**Знать:** Сформированные знания законов, технологии, правил аттестации объекта информатизации. **Уметь:** **С**пособен, но с затруднениями проводить аттестацию объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации. **Владеть:** Основными навыками разработки технологической и эксплуатационной документации.	**Знает:** Глубокие знания законов, технологии, правил аттестации объекта информатизации. **Умеет:** Уверенно проводить аттестацию объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации. **Владеет:** Уверенными навыками разработки технологической и эксплуатационной документации.
ПК-6/ завершающий	*1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.2. программы практики* *2.Качество освоенных обучающимся знаний, умений, навыков*	**Знать:** Поверхностные знания номенклатуры современных программно-аппаратных и технических средств защиты информации; назначения, организации и принципов функционировании программно-аппаратных средств защиты информации; механизмов защиты объек-	**Знать:** Сформированные знания номенклатуры современных программно-аппаратных и технических средств защиты информации; назначения, организации и принципов функционировании программно-аппаратных средств защиты информации; механизмов защиты объек-	**Знает:** Глубокие знания номенклатуры современных программно-аппаратных и технических средств защиты информации; назначения, организации и принципов функционировании программно-аппаратных средств защиты информации; механизмов защиты объек-

Код компетенции/ этап *(указывается название этапа из п.6.1)*	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
	3.Умение применять знания, умения, навыки в типовых и нестандартных ситуаци-ях	тов, реализованные программно-аппаратных средств защиты информации; способов, методов и технических средств защиты конфиденциальной информации; основных положений РД по защите информации на объектах защиты. **Уметь:** Испытывает затруднения при сопоставлении структурной и функциональной организации программных и аппаратных средств защиты информации требованиям политики безопасности; анализе механизмов реализации методов защиты конкретных объектов и процессов для решения профессиональных задач; выявлении уязвимости в эксплуатируемых технических средствах защиты информации. **Владеть:** Элементарными навыками реализации требуемых политик безопасности с помощью современных программно-аппаратных	тов, реализованные программно-аппаратных средств защиты информации; способов, методов и технических средств защиты конфиденциальной информации; основных положений РД по защите информации на объектах защиты. **Уметь:** **С**пособен, но с затруднениями сопоставлять структурную и функциональную организацию программных и аппаратных средств защиты информации требованиям политики безопасности; анализировать механизмы реализации методов защиты конкретных объектов и процессов для решения профессиональных задач; выявлять уязвимости в эксплуатируемых технических средствах защиты информации. **Владеть:** Основными навыками реализации требуемых политик безопасности с помощью современных программно-аппаратных средств	тов, реализованные программно-аппаратных средств защиты информации; способов, методов и технических средств защиты конфиденциальной информации; основных положений РД по защите информации на объектах защиты. **Умеет:** Уверенно сопоставлять структурную и функциональную организацию программных и аппаратных средств защиты информации требованиям политики безопасности; анализировать механизмы реализации методов защиты конкретных объектов и процессов для решения профессиональных задач; выявлять уязвимости в эксплуатируемых технических средствах защиты информации. **Владеет:** Уверенными навыками реализации требуемых политик безопасности с помощью современных программно-аппаратных средств защиты информа-

Код компетенции/ этап *(указывается название этапа из п.6.1)*	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
		средств защиты информации, проведения проверок работоспособности и эффективности применения программно-аппаратных и технических средств защиты информации.	защиты информации, проведения проверок работоспособности и эффективности применения программно-аппаратных и технических средств защиты информации.	ции, проведения проверок работоспособности и эффективности применения программно-аппаратных и технических средств защиты информации.
ПСК-4.2/ завершающий	*1.Доля освоенных обучающимся знаний, умений, навыков от общего объема ЗУН, установленных в п.2. программы практики* *2.Качество освоенных обучающимся знаний, умений, навыков* *3.Умение применять знания, умения, навыки в типовых и нестандартных ситуаци-ях*	**Знать:** Поверхностные знания принципов построения современных операционных систем; особенностей организации средств защиты в распределенных СУБД; назначения, организации и принципов функционировании файловых систем; механизмов защиты информационно-вычислительных сетей, реализованных средствами операционных систем и дополнительного программного обеспечения. **Уметь:** Испытывает затруднения при администрировании подсистемы управления доступа современных операционных систем и программно-аппаратных средств защиты ин-	**Знать:** Сформированные знания принципов построения современных операционных систем; особенностей организации средств защиты в распределенных СУБД; назначения, организации и принципов функционировании файловых систем; механизмов защиты информационно-вычислительных сетей, реализованных средствами операционных систем и дополнительного программного обеспечения. **Уметь:** **С**пособен, но с затруднениями администрировать подсистемы управления доступа современных операционных систем и программно-аппаратные средства защиты инфор-	**Знает:** Глубокие знания принципов построения современных операционных систем; особенностей организации средств защиты в распределенных СУБД; назначения, организации и принципов функционировании файловых систем; механизмов защиты информационно-вычислительных сетей, реализованных средствами операционных систем и дополнительного программного обеспечения. **Умеет:** Способен уверенно администрировать подсистемы управления доступа современных операционных систем и программно-аппаратные средства защиты информации; пользоваться средствами

Код компетенции/ этап *(указывается название этапа из п.6.1)*	Показатели оценивания компетенций	Критерии и шкала оценивания компетенций		
		Пороговый уровень («удовлетворительно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
1	2	3	4	5
		формации; пользовании средствами защиты, предоставляемыми СУБД; установке и настройке операционных систем и их подсистем обеспечения информационной безопасности. **Владеть:** Элементарными навыками работы администратора по защите в базе данных; реализации требуемых политик безопасности средствами операционных систем; оценки эффективности работы операционной системы и её подсистем обеспечения информационной безопасности; администрирования клиентских операционных систем; использования комплексов управления информационной безопасностью с учетом особенностей объектов защиты; восстановления данных.	мации; пользоваться средствами защиты, предоставляемыми СУБД; устанавливать и настраивать операционные системы и их подсистемы обеспечения информационной безопасности. **Владеть:** Основными навыками работы администратора по защите в базе данных; реализации требуемых политик безопасности средствами операционных систем; оценки эффективности работы операционной системы и её подсистем обеспечения информационной безопасности; администрирования клиентских операционных систем; использования комплексов управления информационной безопасностью с учетом особенностей объектов защиты; восстановления данных.	защиты, предоставляемыми СУБД; устанавливать и настраивать операционные системы и их подсистемы обеспечения информационной безопасности. **Владеет:** Уверенными навыками работы администратора по защите в базе данных; реализации требуемых политик безопасности средствами операционных систем; оценки эффективности работы операционной системы и её подсистем обеспечения информационной безопасности; администрирования клиентских операционных систем; использования комплексов управления информационной безопасностью с учетом особенностей объектов защиты; восстановления данных.

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Код компетенции/этап формирования компетенции в процессе освоения ОП ВО *(указывается название этапа из п.6.1)*	Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности
ПК-1/ завершающий	Дневник практики. Характеристика руководителя практики от предприятия лидерских качеств обучающегося.
ПК-2/ завершающий	Дневник практики. Отчет о практике.
ПК-3/ завершающий	Характеристика руководителя практики от предприятия лидерских качеств обучающегося. Дневник практики. Отчет о практике.
ПК-4/ завершающий	Дневник практики. Отчет о практике. Доклад обучающегося на промежуточной аттестации (защита отчета о практике).
ПК-5/ завершающий	Дневник практики. Отчет о практике. Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Ответы на вопросы по содержанию практики на промежуточной аттестации.
ПК-6/ завершающий	Дневник практики. Отчет о практике. Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Ответы на вопросы по содержанию практики на промежуточной аттестации.
ПСК-4.2/ завершающий	Дневник практики. Отчет о практике. Доклад обучающегося на промежуточной аттестации (защита отчета о практике). Ответы на вопросы по содержанию практики на промежуточной аттестации.

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций, закрепленных за производственной практикой по получению профессиональных умений и профессионального опыта, осуществляется в форме текущего контроля и промежуточной аттестации.

Текущий контроль проводится в течение практики на месте ее проведения руководителем практики от предприятия.

На зачет обучающийся представляет дневник практики и отчет о практике. Зачет проводится в форме устной защиты отчета о практике.

Таблица 6.4.1 – Шкала оценки отчета о практике и его защиты

№	Предмет оценки	Критерии оценки	Максимальный балл
1	Содержание отчета 10 баллов	Достижение цели и выполнение задач практики в полном объеме	1
		Отражение в отчете всех предусмотренных программой практики видов и форм профессиональной деятельности	1
		Владение актуальными нормативными правовыми документами и профессиональной терминологией	1
		Соответствие структуры и содержания отчета требованиям, установленным в п. 5 настоящей программы	1
		Полнота и глубина раскрытия содержания разделов отчета	1
		Достоверность и достаточность приведенных в отчете данных	1
		Правильность выполнения расчетов и измерений	1
		Глубина анализа данных	1
		Обоснованность выводов и рекомендаций	1
		Самостоятельность при подготовке отчета	1
2	Оформление отчета 2 балла	Соответствие оформления отчета требованиям, установленным в п.5 настоящей программы	1
		Достаточность использованных источников	1
3	Содержание и оформление презентации (графического материала) 4 балла	Полнота и соответствие содержания презентации (графического материала) содержанию отчета	2
		Грамотность речи и правильность использования профессиональной терминологии	2
4	Ответы на вопросы о содержании практики 4 балла	Полнота, точность, аргументированность ответов	4

Баллы, полученные обучающимся, суммируются, соотносятся с уровнем сформированности компетенций и затем переводятся в традиционные оценки.

Таблица 6.4.2 – Соответствие баллов уровням сформированности компетенций и традиционным оценкам

Баллы	Уровень сформированности компетенций	Оценка
18-20	высокий	отлично
14-17	продвинутый	хорошо
10-13	пороговый	удовлетворительно
9 и менее	недостаточный	неудовлетворительно

7 Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики

7.1 Основная литература:

1. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2013. - 384 с.

2. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С. А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб.: Издательство Политехнического университета, 2014. - 322 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=363040

3. Сердюк, В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Электронный ресурс] : учебное пособие / В. А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - М. : Издательский дом Высшей школы экономики, 2015. - 574 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=440285

4. Степанова, Е. Е. Информационное обеспечение управленческой деятельности [Текст] : учебное пособие / Е. Е. Степанова, Н. В. Хмелевская. - М. : Форум, 2004. - 154 с.

7.2 Дополнительная литература:

1) Аверченков, В. И. Аудит информационной безопасности [Электронный ресурс] : учебное пособие для вузов / В. И. Аверченков. - 3-е изд., стереотип. - М. : Флинта, 2016. - 269 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=93245

2) Абрамов, Г. В. Проектирование информационных систем [Электронный ресурс] : учебное пособие / Г. В. Абрамов, И. Медведкова, Л. Коробова. - Воронеж : Воронежский государственный университет инженерных технологий, 2012. - 172 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=141626

3) Древс, Ю. Г. Организация ЭВМ и вычислительных систем [Текст] : учебник / Ю. Г. Древс. - М. : Высшая школа, 2006. - 501 с.

4) Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю. Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. - Режим доступа : http://biblioclub.ru/index.php?page=book&id=276557

5) Куль, Т. П. Операционные системы [Электронный ресурс] : учебное пособие / Т. П. Куль. - Минск : РИПО, 2015. - 312 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=463629

6) Курячий, Г. В. Операционная система UNIX [Электронный ресурс] : методические рекомендации / Г. В. Курячий. - М. : Интернет-Университет Информационных Технологий, 2004. - 288 с. - Режим доступа : http://biblioclub.ru/index.php?page=book&id=233108

7) Лопин, В. Н. Защита информации в компьютерных системах [Текст] : учебное пособие / В. Н. Лопин, И. С. Захаров, А. В. Николаев ; Министерство образования и науки Российской Федерации, Курский государственный технический университет. - Курск : КГТУ, 2006. - 159 с.

8) Мельников, В. В. Защита информации в компьютерных системах [Текст] / В. В. Мельников. - М. : Финансы и статистика, 1997. - 368 с.

9) Олифер, В. Г. Сетевые операционные системы [Текст] : учебное пособие / В. Г. Олифер, Н. А. Олифер. - СПб. : Питер, 2003. - 539 с.

10) Петренко, В .И. Теоретические основы защиты информации [Электронный ресурс] : учебное пособие / В. И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. - 222 с. - Режим доступа : http://biblioclub.ru/index.php?page=book&id=458204

11) Ярочкин, В. И. Безопасность информационных систем [Текст] /В. И. Ярочкин. - М. : Ось-89, 1996. - 320 с.

7.3 Перечень методических указаний

1) Практика. [Электронный ресурс]: методические указания по написанию отчета и защиты практики для студентов всех форм обучения направления подготовки (специальности) 10.00.00 Информационная безопасность/ Юго-Зап. гос. ун-т; сост.: М.О. Таныгин, И.В. Калуцкий – Электрон. текстовые дан. - Курск, 2018. – 40 с.: прилож.5. – Библиогр.: 21 стр.

2) Научно-исследовательская работа студентов. [Электронный ресурс]: методические рекомендации по проведению, содержанию, оформлению и защите отчета НИРС для студентов всех форм обучения направления подготовки (специальности), 10.00.00 Информационная безопасность/ Юго-Зап. гос. ун-т; сост.: М.О. Таныгин, А.Л. Марухленко – Электрон. текстовые дан. - Курск, 2018. – 27 с.: прилож.4. – Библиогр.: 22 стр.

7.4 Перечень ресурсов информационно-телекоммуникационной сети Интернет

1) Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/
3) Сообщество Ubuntu [официальный сайт]. Режим доступа: http://ubuntu.com/
4) Корпорация Microsoft [официальный сайт]. Режим доступа: http://microsoft.com/
5) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru
6) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru

7) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/
8) База данных "Патенты России"

8 Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1) Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»;
2) Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234,
3) Windows 7, договор IT000012385;
4) Oracle Virtualbox (Бесплатная, GNU General Public License);
5) редактор двоичных файлов Free Hex Editor Neo, (Свободное ПО http://www.hhdsoftware.com/free-hex-editor);
6) открытая среда разработки программного обеспечения Lazarus (Свободное ПО http://www.lazarus.freepascal.org/);
7) ОС FreBSD (свободное ПО, лицензия BSD), ОС Ubuntu (Бесплатная, GNU GPLv3);
8) GNS3 - графический симулятор сети (свободное ПО).

9 Описание материально-технической базы, необходимой для проведения практики

Для проведения практики используется оборудование конкретного предприятия (организации, учреждения), на базе которого она проводится. Отделы и лаборатории предприятия (организации, учреждения) должны соответствовать действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении учебных и научно-производственных работ.:

– Учебная аудитория для проведения занятий лекционного типа и лаборатории кафедры информационной безопасности, оснащенные учебной мебелью: столы, стулья для обучающихся; стол, стул для преподавателя; доска. Компьютеры (12 шт) Компьютер NORBEL C239264Ц-AMD/2x8Gb/2TB/DVDRW/LCD 20";
– МФУ CanoniR 2520
– Межсетевой экран Netgear STM150EW-100EUS
– Роутер ASUS WL-520GC
– Маршрутизатор D-Link DFL-860E
– Коммутатор TrendNet TE100-S88E + 8 port 10/100 Switch
– Система виброакустического зашумления «Шорох-2», виброакустический датчик КПВ-2, акустический излучатель OMS -2000
– Подавитель «жучков» и беспроводных видеокамер “BigHunter Spy”
– Комбинированный поисковый прибор “D008”
– Универсальный поисковый прибор "СРМ-700"

- Лазерный дальномер Mettro 60
- Генератор шума Соната-С1

Для проведения промежуточной аттестации по практике необходимо следующее материально-техническое оборудование:

1. Проекционный экран на штативе; Мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/1471024Mb/160Gb/ сумка/ проектор inFocus IN24