

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»
Институт математики, физики и информационных технологий
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:
Директор института



И. Н. Якунина
«20» января 2021 г.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

Б2.П.1 Эксплуатационная практика

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Формы обучения: очная

год набора: 2020

Тамбов, 2021

Автор программы:

Кандидат физико-математических наук, доцент Лопатин Дмитрий Валерьевич

Программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «01» декабря 2016 г. № 1515).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «22» декабря 2020 г. Протокол № 4

СОДЕРЖАНИЕ

1 Общая характеристика и цель ознакомительной практики.....	4
2 Место практики в структуре образовательной программы и планируемые результаты.....	4
3 Структура и содержание ознакомительной практики.....	8
4 Контроль знаний обучающихся и типовые оценочные средства.....	9
5 Учебно-методические рекомендации по практике.....	18
6 Учебно-методическое и информационное обеспечение практики.....	19
7 Материально-техническое, программное обеспечение практики, программное обеспечение, профес	19

1. Общая характеристика и цель практики

Цель практики – приобретение практических навыков и практического опыта, а также формирование следующих компетенций:

ОК-6 Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия

ПК-1 Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

ПК-2 Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач

ПК-3 Способность администрировать подсистемы информационной безопасности объекта защиты

ПК-4 Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

ПК-5 Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

ПК-6 Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

ПК-8 Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов

ПСК-1 Способность проводить анализ угроз информационно-коммуникационного характера

ПСК-2 Способность организовывать технологический процесс защиты информации, передаваемой по компьютерным сетям

Тип практики	Семестр	Способ проведения	Контактная работа	Форма промежуточной аттестация
Эксплуатаци	7	Стационарн	2	Экзамен

Виды и задачи профессиональной деятельности, к которым готовятся обучающиеся в ходе прохождения практики:

- эксплуатационная

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований
- администрирование подсистем информационной безопасности объекта
- участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем

Практика проводится в форме практической подготовки обучающихся.

2. Место практики в структуре образовательной программы и планируемые результаты

2.1. Эксплуатационная практика относится к базовой части учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность (бакалавриат).

Эксплуатационная практика предусмотрена на 4 курсе, 7 семестр.

Эксплуатационная практика базируется на знаниях, полученных обучающимся по дисциплинам базовой части и вариативной части. Компетенции, сформированные у студентов в процессе прохождения эксплуатационной практики, будут необходимы при изучении профильных дисциплин, а также при прохождении преддипломной практики.

Эксплуатационная практика логически связана с такими дисциплинами, как:

ОК-6 - Преддипломная практика, Психология и педагогика

ПК-1 - Адаптационная дисциплина для инвалидов и лиц с ОВЗ "Основы электро и радиоизмерений", Криптографические методы защиты информации, Основы электро- и радиоизмерений, Программно-аппаратные средства защиты информации, Техническая защита информации, Электроника и схемотехника

ПК-2 - Автоматизация деятельности предприятий, Адаптационная дисциплина для инвалидов и лиц с ОВЗ "Автоматизация деятельности предприятия", Алгоритмизация и программирование, Основы программирования в корпоративных информационных системах, Языки программирования

ПК-3 - Техническая защита информации

ПК-4 - Комплексная система защиты информации объектов информатизации

ПК-5 - Аудит и аттестация объектов информатизации

ПК-6 - Программно-аппаратные средства защиты информации

ПК-8 - Аудит и аттестация объектов информатизации, Практика по получению первичных профессиональных умений и навыков, Преддипломная практика

ПСК-1 - Безопасные информационные технологии

ПСК-2 - Компьютерные сети

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

Код по ФГОС ВО	Компетенция	Знания и умения, необходимые для формирования трудового действия / компетенции
ОК-6	Способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	Знает и понимает: Знает и понимает: способы управления социально-экономическими процессами и трудовыми коллективами
		Умеет (способен продемонстрировать): Умеет: использовать основные положения и научные методы в профессиональной деятельности
		Владеет: Владеет: культурой мышления, способностью к восприятию, методами анализа, обобщения информации
ПК-1	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знает и понимает: Знает и понимает: основы работы с программно аппаратными средствами защиты; основные руководящие документы в области инженерно-технической и программно-аппаратной защиты информации
		Умеет (способен продемонстрировать): Умеет (способен продемонстрировать): применять технические и программно-аппаратные средства обработки и защиты информации
		Владеет: Владеет: необходимыми навыками по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.
ПК-2	Способность применять программные средства системного, прикладного и специального назначения,	Знает и понимает: Знает и понимает: языки программирования; описание и назначение программных средств
		Умеет (способен продемонстрировать):

	инструментальные средства, языки и системы программирования для решения профессиональных задач	<p>Умеет (способен продемонстрировать): работать с программными средствами системного, прикладного и специального назначения; решать стандартные задачи профессиональной деятельности с применением ИКТ</p> <p>Владеет:</p> <p>навыками программирования при разработке систем защиты информации</p>
ПК-3	Способность администрировать подсистемы информационной безопасности объекта защиты	<p>Знает и понимает:</p> <p>Знает и понимает: технические каналы утечки информации; технические средства разведки; способы и средства защиты конфиденциальной информации; подсистемы комплексной системы охраны объектов; основы организации работ по инженерно-технической защите информации; основные руководящие документы в области инженерно-технической защиты информации</p> <p>Умеет (способен продемонстрировать):</p> <p>Умеет (способен продемонстрировать): моделировать объекты защиты; выявлять и оценивать угрозы безопасности информации на конкретных объектах</p> <p>Владеет:</p> <p>Владеет: навыками формальной постановки и решения задач инженерно-технической защиты информации; применения полученных знаний на практике</p>
ПК-4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	<p>Знает и понимает:</p> <p>Знает и понимает: принципы теоретического (научного) обоснования вариантов решения, разработки и организации комплексной системы защиты информации предприятия на основе анализа и оценки угроз безопасности информации и каналов ее дестабилизации, основы нормативно-методического и материально-технического обеспечения ее работы</p> <p>Умеет (способен продемонстрировать):</p> <p>Умеет (способен продемонстрировать): определять рациональные меры защиты на объектах и оценивать их эффективность; контролировать эффективность мер инженерно-технической защиты информации</p> <p>Владеет:</p> <p>Владеет: навыками оценки экономической эффективности мер защиты информации</p>
ПК-5	Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	<p>Знает и понимает:</p> <p>Знает основы действующего законодательства РФ, руководящих и нормативных документов ФСТЭК (Гостехкомиссии) России, регламентирующих вопросы защиты информации; сетевые технологии и вопросы организации защиты автоматизированных систем и их компонентов от несанкционированного доступа; порядок подготовки и проведения аттестации объектов информатизации по требованиям ФСТЭК России; порядок проведения сертификационных испытаний средств защиты информации; порядок лицензирования деятельности по защите информации ФСТЭК России.</p> <p>Умеет (способен продемонстрировать):</p>

		<p>Умеет (способен применять) выполнение работы по аттестации объектов информатизации; подготовка объектов информатизации к аттестационным испытаниям; оценка соответствия автоматизированных систем и реализованных в них технических мер требованиям по безопасности информации; выполнение подготовки к проведению сертификации средств защиты информации.</p> <p>Владеет:</p> <p>оформления результатов аттестационных испытаний объектов информатизации в соответствии с требованиями руководящих и нормативных документов</p>
ПК-6	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	<p>Знает и понимает:</p> <p>порядка проведения сертификационных испытаний средств защиты информации</p> <p>Умеет (способен продемонстрировать):</p> <p>выполнять подготовку к проведению сертификации средств защиты информации</p> <p>Владеет:</p> <p>Владеет: разработки необходимых документов для сертификации средств защиты информации; оформления документации по результатам сертификационных испытаний; подготовки необходимых материалов для получения лицензий на деятельность по защите информации</p>
ПК-8	Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	<p>Знает и понимает:</p> <p>Знает перечень технических средств защиты информации из состава учебно-лабораторного фонда по профилю подготовки, а также основ правовых положений в области информационной безопасности и защиты информации.</p> <p>Умеет (способен продемонстрировать):</p> <p>Умеет применять информационно - справочные и поисковые системы для подбора, изучения и обобщения научнотехнической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.</p> <p>Владеет:</p> <p>Владеет навыками работы по формированию необходимой отчетной документации, а также навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.</p>
ПСК-1	Способность проводить анализ угроз информационно-коммуникационного характера	<p>Знает и понимает:</p> <p>Знает: угрозы информационно-коммуникационного характера: интернет-зависимость, вредоносное программное обеспечение, вымогательство и фишинг в сети интернет, инсайд, нежелательный контент, манипулирование сознанием и действиями пользователя. Знает первоочередные и детальные средства борьбы с информационно-коммуникационными угрозами (программные, организационные, юридические, психологические и этические методы).</p> <p>Умеет (способен продемонстрировать):</p>

		<p>Умеет применять методы борьбы с инфокоммуникационными угрозами. Способен проверять сертификаты сетевой безопасности соединения и регистрационную информацию веб сайта. Умеет оценить репутацию сайтов, блокировать рекламу, всплывающие окна, баннеры и другие нежелательные объекты.</p> <p>Владеет:</p> <p>навыками работы с программными средствами антивирусной и комплекс-ной защиты, родительского контроля, блокирования нежелательного контен-та, антифишинговыми плагинами для браузеров.</p>
ПСК-2	Способность организовывать технологический процесс защиты информации, передаваемой по компьютерным сетям	<p>Знает и понимает:</p> <p>Знает современные сетевые технологии, сетевую модель OSI, принцип построения сети малого предприятия, принцип VPN, способен объяснить преобразование адреса и номера порта PAT.</p> <p>Умеет (способен продемонстрировать):</p> <p>Умеет (способен продемонстрировать): самостоятельно настроить подсети на маршрутизаторе, осознанно объяснить значимость настроек обеспечивающих безопасность сети. Умеет настраивать и работать с VPN, SSH, PAT, NAT, TFTP.</p> <p>Владеет:</p> <p>Владеет: навыками конфигурации маршрутизатора методом консольного доступа и с помощью Telnet, SSH и AUX. Способен выполнить настройку беспроводной локальной сети.</p> <p>Может настроить подсети на оборудование и конечных устройствах, может настроить защищенный удалённый доступ к маршрутизатора, настроить VPN, способен объяснить преобразование адреса и номера порта PAT.</p>

3. Структура и содержание практики

3.1. Объем практики составляет 6 з.е. (216 часов), (4 недели).

3.2. Содержание практики

очная форма

Этап	Содержание этапа практики	Количество часов	Формы текущего контроля
7 семестр			
1.	Подготовительный этап. Обзор технологий, являющиеся составной частью сфер науки, техники и производства, охватывающих совокупность проблем, связанных с обеспечением защищенности объектов информатизации	20	Собеседование
2.	Предварительное обследование объекта. Анализ существующих угроз в информационной сфере	89	Отчёт
3.	Проектирование мероприятий по защите. Проектирование мероприятий по обеспечению информационной безопасности объектов различного уровня (система, объект системы, компонент объекта)	89	Отчёт

4.	Ведение и оформление дневника практики	8	Отчёт
5.	Составление и оформление отчета по эксплуатационной практике	10	Отчёт
	Всего	216	

3.3. Индивидуальные задания по практике:

- Принять участие в проведении аттестации объектов, помещений, технических средств, систем, программ и алгоритмов на предмет соответствия требованиям защиты информации
- Произвести администрирование подсистем информационной безопасности объекта
- Произвести сбор и анализ исходных данных для проектирования систем защиты информации
- Произвести сравнительный анализ подсистем по показателям информационной безопасности
- Принять участие в разработке технологической и эксплуатационной документации
- Провести проектные расчеты элементов систем обеспечения информационной безопасности
- Провести предварительные технико-экономические обоснования проектных расчетов

4. Контроль знаний обучающихся и типовые оценочные средства

4.1 Оценка знаний обучающихся в рамках балльно-рейтинговой системы.

Распределение баллов при прохождении практики:

- Выполнение индивидуального задания по практике – 70 баллов,
- Оформление документации по практике – 10 баллов,
- Защита отчета по практике: 20 баллов

Распределение баллов по заданиям:

№	Вид учебной работы	Мак. кол.	Методика начисления баллов
1.	Выполнение индивидуального задания по практике	70	<p>53 - 70 баллов - индивидуальное задание по практике выполнено в полном объеме:</p> <ul style="list-style-type: none"> - студент показал глубокую теоретическую, методическую, профессиональную подготовку; - умело применил полученные знания во время прохождения практики; - ответственно и с интересом относился к своей работе. <p>36 - 52 баллов - индивидуальное задание по практике выполнено в основном объеме:</p> <ul style="list-style-type: none"> - студент демонстрирует достаточно полные знания всех профессиональных областей; - проявил себя как ответственный исполнитель, заинтересованный в результатах работы; - при собеседовании показал достаточный уровень освоения компетенций. <p>0 – 35 баллов - индивидуальное задание по практике выполнено не в полном объеме:</p> <ul style="list-style-type: none"> - студент не проявил глубоких знаний теории и умения применять их на практике; - не способен самостоятельно продемонстрировать практические умения.
2.	Оформление документации по практике	10	<p>8 - 10 баллов - отчет:</p> <ul style="list-style-type: none"> - выполнен в полном объеме и в соответствии с требованиями; - результативность практики представлена в количественной и качественной характеристике; - материал изложен грамотно, доказательно; - свободно используются понятия, термины, формулировки; - выполненные задания соотносятся с формированием компетенций. <p>5 – 7 баллов - отчет:</p> <ul style="list-style-type: none"> - выполнен в полном объеме и в соответствии с требованиями, но с некоторыми неточностями; - грамотно используется профессиональная терминология - четко и ясно; - описывается анализ выполненных заданий, но не всегда четко соотносится с требованиями. <p>0 - 4 баллов - отчет:</p> <ul style="list-style-type: none"> - низкий уровень владения профессиональным стилем речи в изложении; - низкий уровень оформления документации по практике; - низкий уровень владения методической терминологией;

			- носит описательный характер, без элементов анализа; - низкое качество выполнения заданий, направленных на формиро
3.	Защита отчета по практике	20	16 - 20 баллов - защита и содержание презентации в полной мере с - студент на защите демонстрирует ораторские способности, соблю - содержание выступления отличает: логичность изложения матер - на защите показал высокий уровень освоения компетенций. 11 -15 баллов - защита и содержание презентации в достаточной с - студент на защите демонстрирует эмоциональность, умение отве - содержание выступления отличает: логичность изложения матер - на защите показал достаточный уровень освоения компетенций. 0 – 10 баллов - защита и содержание презентации не в полной мер - студент на защите демонстрирует не полный объем знаний по вс - содержание выступления отличает: не полное раскрытие темы, о - на защите показал недостаточный уровень освоения компетенци
	Итого за практ	100	

Студенту выставляется итоговая оценка промежуточной аттестации в 100-балльной шкале и в традиционной четырехбалльной шкале, характеризующая качество освоения студентом полученных знаний, приобретенных умений и владений по практике. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
85 - 100 баллов	Отлично / зачтено
70 - 84 баллов	Хорошо / зачтено
50 - 69 баллов	Удовлетворительно / зачтено
Менее 50	Неудовлетворительно / не зачтено

4.2 Типовые оценочные средства текущего контроля

Отчёт

На данном этапе отчет по практике должен включать в себя:

- результаты выполнения рабочего плана(графика) прохождения практики;

На данном этапе отчет по практике должен включать в себя:

- описание конкретных видов работ (индивидуальных заданий), выполненных практикантом;
- описание задач, которые приходилось решать под руководством руководителя практики от организации по проектирование мероприятий по обеспечению информационной безопасности объекта различного уровня (система, объект системы, компонент объекта).

Составление и оформление отчета по эксплуатационной практике

Конечным этапом прохождения практики является написание отчета о практике. Отчет о практике должен включать в себя:

- краткую характеристику предприятия или учреждения, на котором проходила практика;
- порядок и сроки прохождения практики;
- необходимые сведения о базе практики;
- результаты выполнения рабочего плана(графика) прохождения практики;
- описание конкретных видов работ (индивидуальных заданий), выполненных практикантом;
- описание задач, которые приходилось решать под руководством руководителя практики от организации;
- описание всех видов методов и средств защиты информации, использованных в работе;
- выводы, оценка положения службы защиты информации в структуре организации, личное отношение и оценка полученных знаний и опыта работы на практике.

Отчет по практике

Отчет по мере надобности иллюстрируется рисунками, картами, схемами, чертежами, фотографиями и другими наглядными материалами.

Оптимальный объем отчёта 10 страниц машинописного текста.

По итогам прохождения практики студент должен своевременно представить на кафедру следующую отчетную документацию:

- отчет о прохождении практики и выполнении индивидуальных заданий;
- отзыв-характеристику о своей работе с места прохождения практики.

Наличие правильно оформленных отчетных документов по практике, отражающих приобретенные компетенции в ходе выполнения индивидуальных заданий, является основанием для выставления положительной оценки.

Собеседование

Типовые вопросы собеседования

1. Концептуальные положения организационного обеспечения информационной безопасности.
2. Функции, задачи и особенности службы безопасности объекта.
3. Организация службы безопасности объекта.
4. Биометрические системы идентификации и аутентификации.
5. Парольные подсистемы идентификации и аутентификации личности.
6. Аппаратные устройства идентификации и аутентификации.
7. Понятие об опасном сигнале и их источниках.
8. Основные и вспомогательные технические средства и системы.
9. Высокочастотные и низкочастотные побочные излучения технических средств и систем (ТСС).
10. Паразитные наводки в цепях электропитания, заземления, в токопроводящих конструкциях помещений и зданий.

4.3 Промежуточная аттестация проводится в форме экзамена

По итогам прохождения практики обучающийся должен своевременно представить на кафедру следующую отчетную документацию:

- отчет о прохождении практики и выполнении индивидуальных заданий;
- отзыв-характеристику о своей работе с места прохождения практики.

Наличие правильно оформленных отчетных документов по практике, отражающих приобретенные компетенции в ходе выполнения индивидуальных заданий, является основанием для выставления соответствующей оценки.

4.4. Шкала оценивания промежуточной аттестации

Оценка	Компет	Дескрипторы (уровни) – основные признаки
	ОК-6	Демонстрирует высокий уровень знаний и понимания в способах управления процессами защиты информации и трудовыми коллективами
	ПК-1	Демонстрирует высокий уровень работы с программно-аппаратными средствами защиты; основные руководящие документы в области инженерно-технической и программно-аппаратной защиты информации Эффективно применяет технические и программно-аппаратные средства обработки и защиты информации; Обладает навыками по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств ЗИ

«отлично»
(85 - 100 балл)

ПК-2	<p>Знает и понимает: языки программирования; описание и назначение программных средств</p> <p>Умеет (способен продемонстрировать): работать с программными средствами системного, прикладного и специального назначения, в локальных и глобальных компьютерных сетях; решать стандартные задачи профессиональной деятельности с применением ИКТ</p> <p>Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано. На вопросы отвечает кратко, аргументировано, уверенно, по существу.</p>
ПК-3	<p>Знает и понимает: технические каналы утечки информации; технические средства разведки; способы и средства защиты конфиденциальной информации; подсистемы комплексной системы охраны объектов; основы организации работ по инженерно-технической защите информации; основные руководящие документы в области инженерно-технической защиты информации</p>
ПК-4	<p>Демонстрирует высокий уровень знаний о принципах теоретического (научного) обоснования вариантов решения, разработки и организации комплексной системы защиты информации предприятия на основе анализа и оценки угроз безопасности информации и каналов ее дестабилизации, основы нормативно-методического и материально-технического обеспечения ее работы.</p>
ПК-5	<p>Демонстрирует высокий уровень знаний обосновах действующего законодательства РФ, руководящих и нормативных документов ФСТЭК (Гостехкомиссии) России, регламентирующих вопросы защиты информации; сетевые технологии и вопросы организации защиты автоматизированных систем и их компонентов от несанкционированного доступа; порядок подготовки и проведения аттестации объектов информатизации по требованиям ФСТЭК России</p>
ПК-6	<p>Знает и понимает: порядок проведения сертификационных испытаний средств защиты информации; порядок лицензирования деятельности по защите информации ФСТЭК России.</p> <p>Умеет (способен продемонстрировать): выполнять подготовку к проведению сертификации средств защиты информации</p>
ПК-8	<p>Демонстрирует высокий уровень знаний перечня технических средств защиты информации из состава учебно-лабораторного фонда по профилю подготовки, а также основ правовых положений в области информационной безопасности и защиты информации.</p> <p>Умеет применять информационно - справочные и поисковые системы для подбора, изучения и обобщения научнотехнической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.</p> <p>Отлично владеет навыками работы по формированию необходимой отчетной документации, а также навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.</p>

ПСК-1	Демонстрирует высокий уровень знаний угроз информационно-коммуникационного характера. Анализирует первоочередные и детальные средства борьбы с информационно-коммуникационными угрозами (программные, организационные, юридические, психологические и этические методы). Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано. Свободно ориентируется по темам лекции. Практическое задание выполнено полностью
ПСК-2	Демонстрирует высокий уровень знаний сетевых технологий, отлично знает принцип работы передачи данных сетевой модели OSI, может настроить подсети на оборудование и конечных устройствах, может настроить защищенный удалённый доступ к маршрутизатора, настроить VPN, способен объяснить преобразование адреса и номера порта PAT. Ответ построен логично, материал излагается четко, ясно, хорошим языком, аргументировано. Свободно ориентируется в направлениях исследований в рамках сетевых технологий. Способен продемонстрировать настройки маршрутизатора для нескольких сетей, настройки коммутатора и защищённого подключения SSH. Свободно ориентируется в материале (примеры из практики, таблицы, графики и т.д.), анализирует и обобщает результаты полученных данных в процессе практического задания (настройки маршрутизатора). На вопросы отвечает кратко, аргументировано, уверенно, по существу
ОК-6	Демонстрирует достаточный уровень знаний и понимания в способах управления процессами защиты информации и трудовыми коллективами
ПК-1	Умеет (способен продемонстрировать): основы работы с программно аппаратными средствами защиты; основные руководящие документы в области инженерно-технической и программно-аппаратной защиты информации
ПК-2	Владеет навыками работы с программными средствами системного, прикладного и специального назначения, в локальных и глобальных компьютерных сетях; решать стандартные задачи профессиональной деятельности с применением ИКТ
ПК-3	Обладает высоким уровнем знаний по техническим каналам утечки информации; техническим средствам разведки; способам и средствам защиты конфиденциальной информации; подсистемам комплексной системы охраны объектов; основам организации работ по инженерно-технической защите информации
ПК-4	Демонстрирует достаточный уровень знаний о принципах теоретического (научного) обоснования вариантов решения, разработки и организации комплексной системы защиты информации предприятия на основе анализа и оценки угроз безопасности информации и каналов ее дестабилизации, основы нормативно-методического и материально-технического обеспечения ее работы

«хорошо»
(70 - 84 балла)

ПК-5	Демонстрирует достаточный уровень знаний об основах действующего законодательства РФ, руководящих и нормативных документов ФСТЭК (Гостехкомиссии) России, регламентирующих вопросы защиты информации; сетевые технологии и вопросы организации защиты автоматизированных систем и их компонентов от несанкционированного доступа; порядок подготовки и проведения аттестации объектов информатизации по требованиям ФСТЭК России
ПК-6	Достаточно хорошо знает порядок проведения сертификационных испытаний средств защиты информации; порядок лицензирования деятельности по защите информации ФСТЭК России. Умеет (способен продемонстрировать): выполнять подготовку к проведению сертификации средств защиты информации
ПК-8	Достаточно хорошо владеет знаниями перечня технических средств защиты информации из состава учебно-лабораторного фонда по профилю подготовки, а также основ правовых положений в области информационной безопасности и защиты информации. Умеет применять информационно - справочные и поисковые системы для подбора, изучения и обобщения научнотехнической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности. Владеет навыками работы по формированию необходимой отчетной документации, а также навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.
ПСК-1	Демонстрирует достаточный уровень знаний угроз информационно-коммуникационного характера. Достаточно свободно ориентируется в работе с программными средствами антивирусной и комплексной защиты, родительского контроля, блокирования нежелательного контента, антифишинговыми плагинами для браузеров. Практическое задание выполнено полностью или с незначительными недочетами. Ответ построен кратко, логично, материал излагается хорошим языком. Вопросы, задаваемые преподавателем, не вызывают существенных затруднений
ПСК-2	Демонстрирует достаточный уровень знаний теории сетевых технологий. Анализирует полученные результаты в процессе выполнения практического задания по настройке маршрутизатора, способен выполнить настройку беспроводной локальной сети. В отдельных примерах может выделить категории IP-адресов. Ответ построен логично, материал излагается хорошим языком. Достаточно свободно ориентируется в направлениях исследований в рамках сетевых технологий. Демонстрируется достаточное знание и понимание современного отечественного и зарубежного направления развития информационных и сетевых технологий. Вопросы, задаваемые преподавателем, не вызывают существенных затруднений

«удовлетворите (50 - 69 баллов)	ОК-6	Демонстрирует недостаточный уровень знаний и понимания в способах управления процессами защиты информации и трудовыми коллективами
	ПК-1	Демонстрирует недостаточный уровень знаний по основам работы с программно аппаратными средствами защиты
	ПК-2	Недостаточно хорошо владеет навыками работы с программными средствами системного, прикладного и специального назначения, в локальных и глобальных компьютерных сетях; Ответ не всегда логично выстроен, материал излагается без применения научной терминологии. Вопросы, задаваемые преподавателем, вызывают затруднения
	ПК-3	Обладает невысоким уровнем знаний по техническим каналам утечки информации; техническим средствам разведки; способам и средствам защиты конфиденциальной информации; подсистемам комплексной системы охраны объектов; основам организации работ по инженерно-технической защите информации
	ПК-4	Демонстрирует недостаточный уровень знаний о принципах теоретического (научного) обоснования вариантов решения, разработки и организации комплексной системы защиты информации предприятия на основе анализа и оценки угроз безопасности информации и каналов ее дестабилизации, основы нормативно-методического и материально-технического обеспечения ее работы
	ПК-5	Демонстрирует недостаточный уровень знаний об основах действующего законодательства РФ, руководящих и нормативных документов ФСТЭК (Гостехкомиссии) России, регламентирующих вопросы защиты информации; сетевые технологии и вопросы организации защиты автоматизированных систем и их компонентов от несанкционированного доступа; порядок подготовки и проведения аттестации объектов информатизации по требованиям ФСТЭК России
	ПК-6	Недостаточно хорошо знает порядок проведения сертификационных испытаний средств защиты информации; порядок лицензирования деятельности по защите информации ФСТЭК России. Умеет (способен продемонстрировать): выполнять подготовку к проведению сертификации средств защиты информации
	ПК-8	Демонстрирует посредственный уровень знаний перечня технических средств защиты информации из состава учебно-лабораторного фонда по профилю подготовки, а также основ правовых положений в области информационной безопасности и защиты информации. Не достаточно хорошо владеет навыками работы по формированию необходимой отчетной документации, а также навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.

ПСК-1	<p>Демонстрирует посредственный уровень знаний угроз информационно-коммуникационного характера.</p> <p>Владеет поверхностными знаниями использования программных средств антивирусной и комплексной защиты.</p> <p>Слабо ориентируется в методах борьбы с информационно-коммуникационными угрозами. Не способен проверить сертификаты сетевой безопасности соединения и регистрационную информацию веб сайта. Неуверенно определяет междисциплинарные связи</p> <p>Ответ не всегда логично выстроен, материал излагается без применения научной терминологии. Вопросы, задаваемые преподавателем, вызывают затруднения</p>
ПСК-2	<p>Демонстрирует не достаточный уровень знаний теории сетевых технологий.</p> <p>Плохо ориентируется в уровнях сетевой модели OSI.</p> <p>Не способен произвести простейшую настройку (установку пароля) на маршрутизатора.</p> <p>Неуверенно определяет междисциплинарные связи</p> <p>Ответ не всегда логично выстроен, материал излагается без применения научной терминологии.</p> <p>Слабо ориентируется в направлениях развития сетевых технологий.</p> <p>Демонстрируется не достаточное знание и понимание построение сетевой инфраструктуры и сети в рамках изучения курса.</p> <p>Слабо ориентируется в настройках маршрутизатора и коммутатора.</p> <p>Вопросы, задаваемые преподавателем, вызывают затруднения</p>
ОК-6	Демонстрирует не достаточный уровень знаний и понимания в способах управления процессами защиты информации и трудовыми коллективами
ПК-1	Не обладает знаниями в области программно аппаратных средств защиты. Неуверенно и логически непоследовательно излагает материал. Неправильно отвечает на поставленные вопросы или затрудняется с ответом
ПК-2	Ответ не логично выстроен, материал излагается без применения научной терминологии. Неправильно отвечает на поставленные вопросы или затрудняется с ответом
ПК-3	Не обладает знаниями в области подсистемам комплексной системы охраны объектов; основам организации работ по инженерно-технической защите информации
ПК-4	Демонстрирует низкий уровень знаний о принципах теоретического (научного) обоснования вариантов решения, разработки и организации комплексной системы защиты информации предприятия на основе анализа и оценки угроз безопасности информации и каналов ее дестабилизации, основы нормативно-методического и материально-технического обеспечения ее работы

«неудовлетворительно» (менее 50 баллов)	ПК-5	<p>Демонстрирует не достаточный уровень знаний об основах действующего законодательства РФ, руководящих и нормативных документов ФСТЭК (Гостехкомиссии) России, регламентирующих вопросы защиты информации;</p> <p>Не разбирается в сетевых технологиях и вопросах организации защиты автоматизированных систем и их компонентов от несанкционированного доступа; Не знает порядок подготовки и проведения аттестации объектов информатизации по требованиям ФСТЭК России</p>
	ПК-6	<p>Не знает порядок проведения сертификационных испытаний средств защиты информации; порядок лицензирования деятельности по защите информации ФСТЭК России.</p> <p>Не умеет (не способен продемонстрировать): выполнять подготовку к проведению сертификации средств защиты информации</p>
	ПК-8	<p>Демонстрирует низкий уровень знаний перечня технических средств защиты информации из состава учебно-лабораторного фонда по профилю подготовки, а также основ правовых положений в области информационной безопасности и защиты информации.</p> <p>Не умеет применять информационно - справочные и поисковые системы для подбора, изучения и обобщения научнотехнической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.</p> <p>Не владеет навыками работы по формированию необходимой отчетной документации, а также навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.</p>
	ПСК-1	<p>Демонстрирует слабый уровень знаний угроз информационно-коммуникационного характера. Не может оценить репутацию сайтов, блокировать рекламу, всплывающие окна, баннеры и другие нежелательные объекты.</p> <p>Не умеет применять методы борьбы с информационно-коммуникационными угрозами.</p> <p>Не может выделить междисциплинарные связи.</p> <p>Неуверенно и логически непоследовательно излагает материал.</p> <p>Неправильно отвечает на поставленные вопросы или затрудняется с ответом. Практическое задание не выполнено.</p>
	ПСК-2	<p>Демонстрирует неудовлетворительный уровень знаний сетевых технологий. Не может объяснить принцип построения сети, построение сетевой модели OSI.</p> <p>Не может произвести настройку конечных устройств локальной сети. Неуверенно и логически непоследовательно излагает материал.</p> <p>Не ориентируется в направлениях развития информационных и сетевых технологий.</p> <p>Не может продемонстрировать знание и понимание команд в терминале настройки маршрутизатора или коммутатора.</p> <p>Не способен назвать определения VPN, SSH, PAT, NAT, TFTP.</p> <p>Неправильно отвечает на поставленные вопросы или затрудняется с ответом.</p>

5. Учебно-методические рекомендации по практике

Обязанности обучающихся во время прохождения практики, требования к оценке выполнения ими рабочего плана (графика) практики и усвоению компетенций, формируемых во время практики закреплены в Положении о практике обучающихся, осваивающих образовательные программы высшего образования, реализуемые в ФГБОУ ВО «Тамбовский государственный университет имени Г.Р. Державина», а также в соответствующих методических материалах (Приложение 8 ОП ВО).

6. Учебно-методическое и информационное обеспечение практики

6.1 Основная литература:

1. Лопатин Д. В. Программно-аппаратная защита информации : электрон. учеб. пособие. - Тамбов: [Б. и.], 2014. - 1 электрон. опт. диск (CD-ROM)
2. Лопатин Д. В. Технология информационной безопасности и методология защиты информации : электрон. учеб. пособие. - Тамбов: [Б. и.], 2014. - 1 электрон. опт. диск (CD-ROM)
3. Лопатин Д.В. Компьютерная экспертиза : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
4. Тамб. гос. ун-т им. Г. Р. Державина "Организационно-правовая защита информации" : учеб. метод. пособие. - Тамбов: [Б. и.], 2014. - 1 электрон. опт. диск (CD-ROM)

6.2 Дополнительная литература:

1. Тамб. гос. ун-т им. Г.Р. Державина, Ин-т математики, физики и информатики Комплексная система защиты информации объектов информатизации : учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
2. Лопатин Д. В. Защита от вредоносных программ : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
3. Тамб. гос. ун-т им. Г.Р. Державина "Аттестация объектов информатизации и выделенных помещений" : учеб.-метод. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

6.3 Иные источники:

1. Вопросы образования - <http://www.ecsocman.edu.ru/vo>
2. Федеральный портал «Российское образование» - <http://www.edu.ru/>
3. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» - <http://school-collection.edu.ru/>

7. Материально-техническое обеспечение практики, программное обеспечение и информационные справочные системы

Для проведения практики необходимо следующее материально-техническое обеспечение: рабочее место, содержащее: персональный компьютер, принтер; возможность выхода в сеть Интернет для поиска информации по профильным сайтам и порталам; помещения для самостоятельной работы; учебные аудитории для проведения групповых и индивидуальных консультаций и промежуточной аттестации.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Лицензионное программное обеспечение:

Microsoft Office Профессиональный плюс 2007

Ревизор-1 XP (средство создания модели системы разграничения доступа)

Ревизор-2 XP (программа контроля полномочий доступа к информационным ресурсам)

Secret Net 5.0-С (мобильный вариант)

Secret Net 5.0-С (автономный вариант)

Delphi 2007 for Win32 Professional

CryptonWipe
 CryptonOffice
 Crypton Шифрование
 CryptonFastDisk

Профессиональные базы данных и информационные справочные системы:

1. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
2. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
3. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
4. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>
5. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prilib.ru>
6. Российская национальная библиотека. – URL: <http://nlr.ru>
7. Российская государственная библиотека. – URL: <https://www.rsl.ru>
8. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>

Электронная информационно-образовательная среда

https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz

Взаимодействие преподавателя и студента во время прохождения последним эксплуатационной практики осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.