


МИНОБРНАУКИ РОССИИ  
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ  
КАФЕДРА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

СОГЛАСОВАНО

на заседании Учебно-методической  
комиссии института  
Протокол № 7 от «24» февраля 2021 г.

УТВЕРЖДАЮ

 Директор  
/А.И. Уразова  
«24» февраля 2021 г.

**ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ**

**ПРЕДДИПЛОМНАЯ ПРАКТИКА**  
Б2.В.01.03(Пд)

Уровень высшего образования:  
специалитет

Специальность  
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация  
№5 «Организация и технологии защиты информации (по отраслям)»

Форма обучения  
очная

Для приема: 2021 г.

Уфа - 2021 г.

Составитель: Юнусова Дарья Сергеевна, к.ф.-м.н., старший преподаватель кафедры управления информационной безопасностью

Программа утверждена на заседании ученого совета института, протокол № 7 от «25» февраля 2021 г.

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета института, протокол № 10 от «24» июня 2021 г.

Дополнения и изменения внесены в соответствии с приказом БашГУ № 770 от 09.06.2021 г.

Директор  / А.И. Уразова

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета факультета / института: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

протокол № \_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 201 \_ г.

Декан/ Директор \_\_\_\_\_ / Ф.И.О./

Дополнения и изменения, внесенные программу практики, утверждены на заседании ученого совета факультета / института:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

протокол № \_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 201 \_ г.

Декан/ Директор \_\_\_\_\_ / Ф.И.О./

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета факультета / института: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

протокол № \_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 201 \_ г.

Декан/ Директор \_\_\_\_\_ / Ф.И.О./

## СОДЕРЖАНИЕ

1. Вид и тип практики, способ, формы, место и организация ее проведения .....	4
2. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций.....	4
3. Место практики в структуре образовательной программы.....	6
4. Объем практики .....	6
5. Содержание практики .....	7
6. Форма отчетности по практике .....	7
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике.....	8
8. Перечень учебной литературы и ресурсов сети Интернет, необходимых для проведения практики .....	24
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для прохождения практики, включая профессиональные базы данных и информационные справочные системы.....	29
10. Описание материально-технической базы, необходимой для проведения практики.....	29

## **1. Вид и тип практики, способ, формы, место и организация ее проведения**

1.1. Вид и тип практики: производственная (преддипломная) практика.

1.2. Способ проведения практики:

стационарная

Стационарной является практика, которая проводится в Университете (филиале) либо в профильной организации, расположенной на территории населенного пункта, в котором расположен Университет (филиал) или профильная организация.

выездная

Выездной является практика, которая проводится вне населенного пункта, в котором расположен Университет (филиал). Выездная практика может проводиться в полевой и иных формах. Конкретный способ проведения практики, предусмотренной ОПОП ВО, указывается с учетом требований ФГОС ВО.

1.3. Практика проводится в следующих формах:

дискретно по видам практики

по видам практик – путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения каждого вида (совокупности видов) практики.

1.4. Место проведения практики.

Организация проведения практики, предусмотренной настоящей программой, осуществляется БашГУ на основе договоров с профильными организациями, деятельность которых соответствует профессиональным компетенциям, осваиваемым в рамках образовательной программы.

Практика может быть проведена непосредственно в учебных или иных подразделениях БашГУ.

Студенты, совмещающие обучение с трудовой деятельностью, вправе проходить учебную, производственную, в том числе преддипломную, практики, по месту трудовой деятельности в случаях, если профессиональная деятельность, осуществляемая ими, соответствует требованиям к содержанию практики.

1.5. Руководство практикой.

Для руководства практикой, проводимой в БашГУ, назначается руководитель (руководители) практики от университета из числа лиц, относящихся к профессорско-преподавательскому составу БашГУ.

Для руководства практикой, проводимой в профильной организации, назначается руководитель (руководители) практики из числа работников профильной организации.

1.6. Организация проведения практики.

Направление на практику оформляется приказом БашГУ с указанием вида и/или типа, срока, места прохождения практики, а также данных о руководителях практики из числа лиц, относящихся к профессорско-преподавательскому составу БашГУ.

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

2.1. Основной целью преддипломной практики является:

обобщение знаний и навыков работы студентов по специальности. Преддипломная практика является завершающим этапом подготовки выпускника в сфере защиты информации и проводится для овладения первоначальным профессиональным опытом, проверки профессиональной готовности будущего специалиста к самостоятельной трудовой деятельности и сбора материалов для выполнения выпускной квалификационной работы. Содержание преддипломной практики определяется темой выпускной квалификационной работы.

2.2. Основными задачами преддипломной практики являются:  
 - сбор материала для написания выпускной квалифицированной работы;  
 - овладение профессиональными навыками, методами управления процессами защиты информации на предприятии.

2.3. Перечень индикаторов достижения компетенций с указанием планируемых результатов обучения по практике:

<b>Формируемая компетенция (с указанием кода)</b>	<b>Код и наименование индикатора достижения компетенции</b>	<b>Результаты обучения по практике</b>
УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9-1	Знает экономические и социальные условия и последствия реализации профессиональных решений.
	УК-9-2	Знает принципы и методы экономических наук для решения профессиональных задач.
	УК-9.3	Умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; находить информацию по тематике и выбирать информационные ресурсы и источники знаний в электронной среде; оценивать стоимость владения подсистемой информационной безопасности.
	УК-9.4	Владеет навыками принятия обоснованных различными методами и подходами экономических решений в различных областях жизнедеятельности.
ПК-2. Способен проводить мероприятия по оценке защищенности компьютерных систем и сетей	ИПК-2.1	Знает основные критерии оценки защищенности компьютерных систем и сетей.
	ИПК-2.2	Умеет выявлять и анализировать уязвимости.
	ИПК-2.3	Владеет методами и инструментами оценки защищенности компьютерных систем и сетей.
ПК-3. Способен анализировать защищенность компьютерных систем, проводить проверку	ИПК-3.1	Знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации.

работоспособности и эффективности применяемых средств защиты информации	ИПК-3.2	Умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации.
	ИПК-3.3	Владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации.
ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей	ИПК 1.1	Знает основные требования по защите информации компьютерных систем и сетей
	ИПК 1.2	Умеет формировать требования по защите информации компьютерных систем и сетей
	ИПК 1.3	Владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей
ПК-4. Способен определять основные угрозы безопасности информации в автоматизированных системах	ИПК-4.1	Знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах.
	ИПК-4.2	Умеет определять основные угрозы безопасности информации в автоматизированных системах.
	ИПК-4.3	Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах.

### 3. Место практики в структуре образовательной программы

Преддипломная практика входит в часть, формируемую участниками образовательных отношений образовательной программы специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Практика проводится в соответствии с календарным учебным графиком и ориентирована на закрепление изученных и осваиваемых дисциплин (модулей).

### 4. Объем практики

Учебным планом по специальности 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» предусмотрено проведение практики: общая трудоемкость составляет 6 зачетных единиц (216 академических часов). В том числе: в форме контактной работы 2 часа, в форме самостоятельной работы 214 часов.

## 5. Содержание практики

№	Разделы (этапы) практики	Виды и содержание работ, в т.ч. самостоятельная работа обучающегося	Форма текущего контроля и промежуточная аттестация
1.	Подготовительный этап	Инструктаж по технике безопасности и противопожарной безопасности. Ознакомиться с историей и направлениями развития предприятия (организации).	Запись в журнале инструктажа
2.	Основной этап	Выполнение индивидуального задания, сбор необходимой фактической информации, систематизация литературного материала, изучение документов, характеризующие предприятие (Устав, свидетельства, лицензии, Положения об отделах и службах, Должностные инструкции, Коллективный договор), изучение структуры управления предприятием, состав и взаимосвязь основных его структурных подразделений, описание работы подразделений предприятия, выработка предложений и рекомендаций по итогам прохождения практики.	Результаты выполнения заданий
3.	Заключительный этап	Обработка и анализ полученной информации, подготовка отчета по практике.	Подборка материалов и документов, отчет по практике
	ИТОГО		Дифференцированный зачет с оценкой

## 6. Форма отчетности по практике

В качестве основной формы и вида отчетности для всех форм обучения студентов устанавливается отчет по практике. По окончании практики студент сдает корректно, полно и аккуратно заполненный отчет по практике руководителю практики от соответствующей кафедры.

Промежуточная аттестация по итогам практики может включать защиту отчета в зависимости от требований образовательного стандарта по направлению подготовки (специальности).

Итоговой формой контроля знаний, умений и навыков по практике является дифференцированный зачет с оценкой.

Он служит для оценки работы студента в течение всего периода прохождения практики и призван выявить уровень, прочность и систематичность полученных им теоретических и практических знаний, приобретения профессиональных умений и навыков, умение синтезировать полученные знания и применять их в решении практических задач. Вопросы предполагают контроль общих методических знаний и умений, способность студентов проиллюстрировать их примерами, индивидуальными материалами, составленными студентами в течение практики.

Случаи невыполнения программы практики, получения не удовлетворительной оценки при защите отчета, а также не прохождения практики признаются академической задолженностью.

Академическая задолженность подлежит ликвидации в установленные деканатом (дирекцией) срок.

## **7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике**

### **7.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по практике. Описание критериев и шкал оценивания результатов обучения по практике.**

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности

<b>Код и наименование индикатора достижения компетенции</b>	<b>Результаты обучения по практике</b>	<b>Критерии оценивания</b>	<b>Шкала оценивания</b>
УК-9-1	Знает экономические и социальные условия и последствия реализации профессиональных решений.	Демонстрирует целостные знания о экономических и социальных условиях и последствиях реализации профессиональных решений	отлично
		В целом знает экономические и социальные условия и последствия реализации профессиональных решений	хорошо
		Имеет фрагментарные знания о экономических и социальных условиях и последствиях реализации профессиональных решений	удовлетворительно
		Не знает экономические и социальные условия и последствия реализации	неудовлетворительно



		профессиональн х решений	
УК-9-2	Знает принципы и методы экономических наук для решения профессиональных задач.	Демонстрирует целостные знания о принципах и методах экономических наук для решения профессиональн х задач	отлично
		В целом знает принципы и методы экономических наук для решения профессиональн х задач	хорошо
		Имеет фрагментарные знания о принципах и методах экономических наук для решения профессиональн х задач	удовлетворительно
		Не знает принципы и методы экономических наук для решения профессиональн х задач	неудовлетворитель но
УК-9.3	Умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; находить информацию по тематике и выбирать информационные ресурсы и источники знаний в электронной среде; оценивать стоимость владения	Умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; находить информацию по тематике и выбирать информационные ресурсы и источники знаний в электронной среде; оценивать стоимость	отлично

	подсистемой информационной безопасности.	владения подсистемой информационной безопасности.	
		Умеет находить информацию по тематике и выбирать информационные ресурсы и источники знаний в электронной среде; оценивать стоимость владения подсистемой информационной безопасности, но не умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения	хорошо
		Умеет находить информацию по тематике и выбирать информационные ресурсы и источники знаний в электронной среде, но не умеет оценивать стоимость владения подсистемой информационной безопасности, а также оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения	удовлетворительно

		Не умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; находить информацию по тематике и выбирать информационные ресурсы и источники знаний в электронной среде; оценивать стоимость владения подсистемой информационной безопасности	неудовлетворительно
УК-9.4	Владеет навыками принятия обоснованных различными методами и подходами экономических решений в различных областях жизнедеятельности.	Владеет навыками принятия обоснованных различными методами и подходами экономических решений в различных областях жизнедеятельности	отлично
		В целом владеет навыками принятия обоснованных различными методами и подходами экономических решений в различных областях жизнедеятельности, но допускает незначительные ошибки	хорошо
		В целом владеет	удовлетворительно

		<p>навыками принятия обоснованных различными методами и подходами экономических решений в различных областях жизнедеятельности, но допускает значительные ошибки</p>	
		<p>Не владеет навыками принятия обоснованных различными методами и подходами экономических решений в различных областях жизнедеятельности</p>	<p>неудовлетворительно</p>

ПК-2. Способен проводить мероприятия по оценке защищенности компьютерных систем и сетей

<b>Код и наименование индикатора достижения компетенции</b>	<b>Результаты обучения по практике</b>	<b>Критерии оценивания</b>	<b>Шкала оценивания</b>
ИПК-2.1	Знает основные критерии оценки защищенности компьютерных систем и сетей.	Знает основные критерии оценки защищенности компьютерных систем и сетей	отлично
		В целом знает основные критерии оценки защищенности компьютерных систем и сетей	хорошо
		Имеет фрагментарные знания об	удовлетворительно

		основных критериях оценки защищенности компьютерных систем и сетей	
		Не знает основные критерии оценки защищенности компьютерных систем и сетей	неудовлетворительно
ИПК-2.2	Умеет выявлять и анализировать уязвимости.	Умеет выявлять и анализировать уязвимости	отлично
		В целом умеет выявлять и анализировать уязвимости	хорошо
		Не показывает сформированного умения выявлять и анализировать уязвимости	удовлетворительно
		Не умеет выявлять и анализировать уязвимости	неудовлетворительно
ИПК-2.3	Владеет методами и инструментами оценки защищенности компьютерных систем и сетей.	Владеет методами и инструментами оценки защищенности компьютерных систем и сетей	отлично
		Владеет методами и инструментами оценки защищенности компьютерных систем и сетей, но допускает незначительные ошибки	хорошо
		Владеет методами и инструментами оценки защищенности компьютерных систем и сетей, но допускает значительные ошибки	удовлетворительно
		Не владеет	неудовлетворительно

		методами и инструментами оценки защищенности компьютерных систем и сетей	но
--	--	--	----

ПК-3. Способен анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации

<b>Код и наименование индикатора достижения компетенции</b>	<b>Результаты обучения по практике</b>	<b>Критерии оценивания</b>	<b>Шкала оценивания</b>
ИПК-3.1	Знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации.	Знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	отлично
		В целом знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	хорошо
		Имеет фрагментарные знания об основных принципах и методах анализа защищенности	удовлетворительно

		компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	
		Не знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	неудовлетворительно
ИПК-3.2	Умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации.	Умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации	отлично
		Умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации, но допускает незначительные ошибки	хорошо

		<p>Умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации, но допускает значительные ошибки</p>	удовлетворительно
		<p>Не умеет анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации</p>	неудовлетворительно
ИПК-3.3	<p>Владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации.</p>	<p>Владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации</p>	отлично
		<p>В целом владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения</p>	хорошо



		проверки работоспособности и эффективности применяемых средств защиты информации	
		Владеет использованием основных принципов и методов анализа защищенности компьютерных систем, но не владеет навыками проведения проверки работоспособности и эффективности применяемых средств защиты информации	удовлетворительно
		Не владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	неудовлетворительно

ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей

<b>Код и наименование индикатора достижения компетенции</b>	<b>Результаты обучения по практике</b>	<b>Критерии оценивания</b>	<b>Шкала оценивания</b>
ИПК 1.1	Знает основные требования по защите	Знает основные требования по	отлично

	информации компьютерных систем и сетей	защите информации компьютерных систем и сетей	
		В целом знает основные требования по защите информации компьютерных систем и сетей	хорошо
		Имеет фрагментарные знания об основных требованиях по защите информации компьютерных систем и сетей	удовлетворительно
		Не знает основные требования по защите информации компьютерных систем и сетей	неудовлетворительно
ИПК 1.2	Умеет формировать требования по защите информации компьютерных систем и сетей	Умеет формировать требования по защите информации компьютерных систем и сетей	отлично
		Умеет формировать требования по защите информации компьютерных систем и сетей, но допускает незначительные ошибки	хорошо
		Умеет формировать требования по защите информации компьютерных систем и сетей, но допускает	удовлетворительно

		значительные ошибки	
		Не умеет формировать требования по защите информации компьютерных систем и сетей	неудовлетворительно
ИПК 1.3	Владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей	Владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей	отлично
		В целом владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей	хорошо
		Владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей, но допускает значительные ошибки	удовлетворительно
		Не владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей	неудовлетворительно

ПК-4. Способен определять основные угрозы безопасности информации в автоматизированных системах

Код и наименование индикатора достижения компетенции	Результаты обучения по практике	Критерии оценивания	Шкала оценивания
ИПК-4.1	Знает принципы и методы определения основных угроз безопасности информации в автоматизированных системах.	Знает принципы и методы определения основных угроз безопасности информации в автоматизированных системах	отлично
		В целом знает принципы и методы определения основных угроз безопасности информации в автоматизированных системах	хорошо
		Имеет фрагментарные знания о принципах и методах определения основных угроз безопасности информации в автоматизированных системах	удовлетворительно
		Не знает принципы и методы определения основных угроз безопасности информации в автоматизированных системах	неудовлетворительно
ИПК-4.2	Умеет определять основные угрозы безопасности информации в автоматизированных	Умеет определять основные угрозы безопасности информации в автоматизированных	отлично

	системах.	ых системах	
		Умеет определять основные угрозы безопасности информации в автоматизированных системах, но допускает незначительные ошибки	хорошо
		Умеет определять основные угрозы безопасности информации в автоматизированных системах, но допускает значительные ошибки	удовлетворительно
		Не умеет определять основные угрозы безопасности информации в автоматизированных системах	неудовлетворительно
ИПК-4.3	Владеет принципами и методами определения основных угроз безопасности информации в автоматизированных системах.	Владеет принципами и методами определения основных угроз безопасности информации в автоматизированных системах	отлично
		Уверенно владеет принципами и методами определения основных угроз безопасности информации в автоматизированных системах, но допускает незначительные ошибки	хорошо
		Владеет принципами и методами определения основных угроз	удовлетворительно

		безопасности информации в автоматизированных системах, но допускает значительные ошибки	
		Не владеет принципами и методами определения основных угроз безопасности информации в автоматизированных системах	неудовлетворительно

**7.2. Типовые контрольные вопросы (задания) или иные материалы, необходимые для оценивания результатов обучения по практике. Методические материалы, определяющие процедуры оценивания результатов обучения по практике.**

Варианты возможных тем индивидуальных заданий:

1. Организация безопасного удаленного доступа к ЛВС организации.
2. Построение защищенной виртуальной сети на базе специализированного программного обеспечения в организации.
3. Автоматизация учета конфиденциальных документов в организации.
4. Организация процессов мониторинга конфиденциального документооборота в организации.
5. Автоматизация процесса проверок наличия конфиденциальных документов в организации.
6. Разработка комплексной системы защиты информации (КСЗИ) организации.
7. Организация системы планирования и контроля функционирования КСЗИ в организации.
8. Разработка основных направлений совершенствования КСЗИ организации.
9. Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации в организации.
10. Разработка методологии проектирования КСЗИ.
11. Разработка моделей процессов защиты информации при проектировании КСЗИ.
12. Анализ методов оценки качества функционирования КСЗИ.
13. Разработка структурно-функциональной модели управления КСЗИ организации.
14. Разработка проекта программно-аппаратной защиты информации организации.
15. Разработка методов расчета экономической эффективности программно-аппаратной защиты информации организации.
16. Криптографические средства защиты информации на основе дискретных носителей.
17. Разработка игровой (дискретной) модели программно-аппаратной защиты информации организации.
18. Обоснование и разработка требований и процедур по защите информации ограниченного доступа в организации.
19. Анализ нормативно-правовой базы по защите информации в сети Интернет. Разработка требований по организационной защите конфиденциальной информации,

передаваемой и получаемой по сети Интернет.

20. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников организации со сторонними организациями.

Примерные вопросы к зачету:

1. Каковы назначение, цели деятельности, структура учреждения (предприятие, организация), в которой проходила практика?
2. На основании каких учредительных документов функционирует данное учреждение (предприятие, организация)?
3. Какими основными нормативно-правовыми актами руководствуется в своей деятельности данное учреждение (предприятие, организация)?
4. Какие организационные, инженерно-технические, программно-аппаратные меры защиты информации применяются в учреждении (предприятии, организации), в которой проходила практика?
5. Какая информация является конфиденциальной для учреждения (предприятия, организации), в которой проходила практика?
6. Какие знания, умения и навыки были приобретены или развиты в результате прохождения практики?
7. Какие задания были выполнены в ходе прохождения практики?
8. Какие документы (проекты документов) были составлены?
9. Какая литература была изучена по теме выпускной квалификационной работы?
10. Какие материалы были собраны для практической части выпускной квалификационной работы?

Студент на зачет должен представить:

- отчет, подписанный руководителем практики от кафедры и предприятия;
- материалы, связанные с выполнением индивидуального задания и программы практики.

Оценка по итогам прохождения практики и защиты отчета проставляется в ведомость в виде дифференцированного зачета с оценкой.

### **Шкала оценивания для промежуточной аттестации обучающихся по практике**

Оценка «отлично» выставляется, если студент выполнил план прохождения практики, осуществил подборку необходимых нормативных правовых документов учреждения (организации, предприятия), умело анализирует полученный во время практики материал, решения и действия должностных лиц, правильно оценивает их с точки зрения законности и обоснованности, свободно отвечает на все вопросы по существу, правильно оформил отчет о практике, имеет положительный отзыв-характеристику с места практики.

Оценка «хорошо» выставляется, если студент выполнил план прохождения практики, осуществил подборку необходимых нормативных правовых документов учреждения (организации, предприятия), анализирует полученный во время практики материал, решения и действия должностных лиц, относительно правильно оценивает их с точки зрения законности и обоснованности, отвечает на вопросы по существу, оформил отчет о практике с незначительными недостатками, имеет положительный отзыв-характеристику с места практики.

Оценка «удовлетворительно» выставляется, если студент выполнил план прохождения практики, не в полном объеме осуществил подборку необходимых нормативных правовых документов учреждения (организации, предприятия), недостаточно четко и правильно анализирует полученный во время практики материал,

решения и действия должностных лиц, не всегда правильно оценивает их с точки зрения законности и обоснованности, отвечает на вопросы не по существу, оформил отчет о практике с недостатками, имеет отзыв-характеристику с места практики с указанием отдельных недостатков.

Оценка «неудовлетворительно» выставляется, если студент не выполнил план прохождения практики, не осуществил подборку необходимых нормативных правовых документов учреждения (организации, предприятия), не правильно анализирует полученный во время практики материал, решения и действия должностных лиц, не правильно оценивает их с точки зрения законности и обоснованности, не отвечает на вопросы по существу, не правильно оформил отчет о практике, имеет отрицательный отзыв-характеристику с места практики.

Студент, не выполнивший программу практики, и получивший оценку «неудовлетворительно» считается не прошедшим практику.

Студенты, не выполнившие программу практики без уважительной причины или получившие отрицательную оценку, могут быть отчислены из вуза как имеющие академическую задолженность.

Студенты, не выполнившие программу практики по уважительной причине, направляются на практику вторично в свободное от учебы время.

## **8. Перечень учебной литературы и ресурсов сети Интернет, необходимых для проведения практики**

### **8.1. Основная литература**

1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>.

2. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - Москва: Горячая линия-Телеком, 2015. - 585 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0424-8; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=457143>.

3. Малюк, А.А. Теория защиты информации / А.А. Малюк. - Москва: Горячая линия - Телеком, 2012. - 184 с.: ил. - Библиогр. в кн. - ISBN 978-5-9912-0246-6; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=253553>.

4. Лукаш, Ю.А. Контроль персонала как составляющая безопасности и развития бизнеса: учебное пособие / Ю.А. Лукаш. - 2-е изд., стер. - Москва: Издательство «Флинта», 2017. - 24 с. - ISBN 978-5-9765-1377-8; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=115078>.

5. Бурькова, Е.В. Физическая защита объектов информатизации: учебное пособие / Е.В. Бурькова; Министерство образования и науки Российской Федерации, Оренбургский Государственный Университет, Кафедра вычислительной техники и защиты информации. - Оренбург: Оренбургский государственный университет, 2017. - 158 с.: табл., схем. - Библиогр. в кн. - ISBN 978-5-7410-1697-8; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=481730>.

6. Пожарная и охранно-пожарная сигнализация / сост. С.В. Собурь. - 3-е изд., перераб. - Москва: ПожКнига, 2010. - 336 с. - (Системы комплексной безопасности). - ISBN 978-5-98629-028-7; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=140300>.

7. Пожарная и охранно-пожарная сигнализация: проектирование, монтаж, эксплуатация и обслуживание: справочник / сост. С.В. Собурь ; под ред. М.М.Любимова; Всемирная академия наук комплексной безопасности, Международная ассоциация «Системсервис» и др. - 4 -е изд., с изм. - Москва: ПожКнига, 2014. - 256 с.: табл. -



- (Системы комплексной безопасности). - Библиогр. в кн. - ISBN 978-5-98629-052-2; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=479740>
8. Ворона, В.А. Технические системы охранной и пожарной сигнализации / В.А. Ворона, В.А. Тихонов. - Москва: Горячая линия - Телеком, 2012. - 376 с.: ил. - (Обеспечение безопасности объектов; Вып. 5). - Библиогр. в кн. - ISBN 978-5-9912-0192-6; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=253102>.
9. Собоурь, С.В. Установки пожарной сигнализации / С.В. Собоурь. - 6-е изд., перераб. - Москва: ПожКнига, 2012. - 296 с. - («Пожарная безопасность предприятия»). - ISBN 978-5-98629-040-9; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=236598>.
10. Собоурь, С.В. Пожарная безопасность электроустановок / С.В. Собоурь. - 9-е изд., перераб., с изм. - Москва: ПожКнига, 2013. - 272 с. - («Пожарная безопасность предприятия»). - ISBN 978-5-98629-051-5; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=236599>.
11. Организация безопасной работы информационных систем: учебное пособие / Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др.; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=277794>.
12. Пескин, А.Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации / А.Е. Пескин. - Москва: Горячая линия - Телеком, 2013. - 256 с.: ил. - Библиогр. в кн. - ISBN 978-5-9912-0336-4; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=253583>.
13. Системы безопасности: журнал для руководителей и специалистов в области безопасности / ред. О. Федосеева - Москва : ГРОТЕК, 2014. - № 3(117). - 182 с.: ил.; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=238448>.
14. Петренко, В.И. Теоретические основы защиты информации: 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.: ил. - Библиогр.: с. 214-215; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=458204>.
15. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стер. - Москва: Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93245>.
16. Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва: Издательство «Флинта», 2016. - 224 с. - (Организация и технология защиты информации). - Библиогр.: с. 192-193. - ISBN 978-5-9765-1274-0; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93351>.
17. Аудит информационной безопасности органов исполнительной власти: учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувьклин, М.В. Рудановский. - 4-е изд., стер. - Москва: Издательство «Флинта», 2016. - 100 с. - (Организация и технология защиты информации). - Библиогр.: с. 83-84. - ISBN 978-5-9765-1277-1; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93259>.
18. Малюк, А.А. Защита информации в информационном обществе: учебное пособие / А.А. Малюк. - Москва: Горячая линия-Телеком, 2015. - 229 с.: ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0481-1; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=457170>.

19. Аверченков, В.И. История развития системы государственной безопасности России: учебное пособие / В.И. Аверченков, В.В. Ерохин, О.М. Голембиовская. - 3-е изд., стер. - Москва: Издательство «Флинта», 2016. - 192 с. - Библиогр. в кн. - ISBN 978-5-9765-1259-7; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93267>.
20. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие / В.А. Сердюк; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва: Издательский дом Высшей школы экономики, 2015. - 574 с.: ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=440285>.
21. Дашков, Л.П. Организация и управление коммерческой деятельностью: учебник / Л.П. Дашков, О.В. Памбухчиянц. - 2-е изд., перераб. - Москва: Издательско-торговая корпорация «Дашков и К°», 2018. - 400 с. : ил. - (Учебные издания для бакалавров). - ISBN 978-5-394-02531-0; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=495757>.
22. Плашенко, В. Обеспечение безопасности бизнеса промышленных предприятий: теория и практика: учебное пособие / В. Плашенко; науч. ред. А.Н. Зуев; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «ЧЕРЕПОВЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ», Институт информационных технологий. - Череповец: Издательство ЧГУ, 2014. - 331 с.: ил., табл. - Библиогр. в кн. - ISBN 978-5-85341-634-5; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=434840>.
23. Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - Москва: Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93356>.
24. Милославская, Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва: Горячая линия - Телеком, 2013. - 216 с.: ил. - (Вопросы управления информационной безопасностью. Вып. 4). - Библиогр. в кн. - ISBN 978-5-9912-0274-9; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=253578>.
25. Организация безопасной работы информационных систем: учебное пособие / Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др.; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=277794> .
26. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности: учебное пособие / Ю.И. Коваленко. - Москва: Горячая линия - Телеком, 2012. - 140 с.: ил. - Библиогр. в кн. - ISBN 978-5-9912-0261-9; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=253538>.
27. Смирнов, А.А. Обеспечение информационной безопасности в условиях виртуализации общества: опыт Европейского Союза: монография / А.А. Смирнов. - Москва: ЮНИТИ-ДАНА: Закон и право, 2012. - 159 с.: ил. - (Научные издания для юристов). - Библиогр. в кн. - ISBN 978-5-238-02259-8; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=448202>.
28. Обеспечение информационной безопасности бизнеса / В.В. Андрианов, С.Л. Зефирова, В.Б. Голованов, Н.А. Голдуев; ред. А.П. Курило. - 2-е изд., перераб. и доп. -

Москва: Альпина Паблишерз, 2011. - 373 с. - ISBN 978-5-9614-1364-9; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=235577>.

29. Инструментальный контроль и защита информации: учебное пособие / Н.А. Свиначев, О.В. Ланкин, А.П. Данилкин и др.; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». - Воронеж: Воронежский государственный университет инженерных технологий, 2013. - 192 с.: табл., ил. - Библиогр. в кн. - ISBN 978-5-00032-018-1; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=255905>

30. Титов, А.А. Инженерно-техническая защита информации: учебное пособие / А.А. Титов. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. - 195 с.; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=208567>.

31. Милославская, Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса: учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва: Горячая линия - Телеком, 2013. - 170 с.: ил. - (Вопросы управления информационной безопасностью. Вып. 3). - Библиогр. в кн. - ISBN 978-5-9912-0273-2; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=253577>.

32. Методологические основы построения защищенных автоматизированных систем: учебное пособие / А.В. Душкин, О.В. Ланкин, С.В. Потехецкий и др.; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». - Воронеж: Воронежская государственная лесотехническая академия, 2013. - 258 с.: табл., ил. - Библиогр. в кн. - ISBN 978-5-89448-981-0; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=255851>

## 8.2. Дополнительная литература

33. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс]: учебное пособие / В.Ф. Шаньгин. - Электрон. дан. - Москва: ДМК Пресс, 2012. - 592 с. - Режим доступа: <https://e.lanbook.com/book/3032>. - Загл. с экрана.

34. Савельев, А.И. Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (постатейный) [Электронный ресурс] / А.И. Савельев. - Электрон. дан. - Москва: СТАТУТ, 2015. - 320 с. - Режим доступа: <https://e.lanbook.com/book/75062>. - Загл. с экрана.

35. Симонис, Д. Check Point NG. Руководство по администрированию [Электронный ресурс]: руководство / Д. Симонис, К.С. Пинкок, Д. Клигерман. - Электрон. дан. - Москва: ДМК Пресс, 2008. - 544 с. - Режим доступа: <https://e.lanbook.com/book/1078>. - Загл. с экрана.

36. Петренко, В.И. Защита персональных данных в информационных системах. Практикум [Электронный ресурс]: учебное пособие / В.И. Петренко, И.В. Мандрица. - Электрон. дан. - Санкт-Петербург: Лань, 2019. - 108 с. - Режим доступа: <https://e.lanbook.com/book/111916>. - Загл. с экрана.

37. Юсупов, Р.Х. Основы автоматизированных систем управления технологическими процессами [Электронный ресурс]: учебное пособие / Р.Х. Юсупов. - Электрон. дан. - Вологда: «Инфра-Инженерия», 2018. - 132 с. - Режим доступа: <https://e.lanbook.com/book/108630>. - Загл. с экрана.

38. Никифоров, С.Н. Методы защиты информации. Защита от внешних вторжений [Электронный ресурс] : учеб. пособие / С.Н. Никифоров. - Электрон. дан. - Санкт-Петербург: Лань, 2018. - 96 с. - Режим доступа: <https://e.lanbook.com/book/107306>. - Загл. с экрана.

39. Широков, Ю.А. Управление промышленной безопасностью [Электронный ресурс] : учебное пособие / Ю.А. Широков. - Электрон. дан. - Санкт-Петербург: Лань,

2019. - 360 с. - Режим доступа: <https://e.lanbook.com/book/112683>. - Загл. с экрана.
40. Ехлаков, Ю.П. Управление программными проектами. Стандарты, модели [Электронный ресурс]: учебное пособие / Ю.П. Ехлаков. - Электрон. дан. - Санкт-Петербург : Лань, 2019. - 244 с. - Режим доступа: <https://e.lanbook.com/book/111914>. - Загл. с экрана.
41. Свечин А.А., Стратегия [Электронный ресурс] / Свечин А.А.. - Электрон. дан. - Санкт-Петербург: Лань, 2013. - 297 с. - Режим доступа: <https://e.lanbook.com/book/9848>. - Загл. с экрана.
42. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] / А.А. Бирюков. - Электрон. дан. - Москва: ДМК Пресс, 2017. - 434 с. - Режим доступа: <https://e.lanbook.com/book/93278>. - Загл. с экрана.
43. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] : учебник / А.А. Бирюков. - Электрон. дан. - Москва: ДМК Пресс, 2012. - 474 с. - Режим доступа: <https://e.lanbook.com/book/39990>. - Загл. с экрана.
44. Масалков, А.С. Особенности киберпреступлений: инструменты нападения и защиты информации [Электронный ресурс] / А.С. Масалков. - Электрон. дан. - Москва : ДМК Пресс, 2018. - 226 с. - Режим доступа: <https://e.lanbook.com/book/105842>. - Загл. с экрана.
45. Никифоров, С.Н. Методы защиты информации. Защита от внешних вторжений [Электронный ресурс] : учеб. пособие / С.Н. Никифоров. - Электрон. дан. - Санкт-Петербург: Лань, 2018. - 96 с. - Режим доступа: <https://e.lanbook.com/book/107306>. - Загл. с экрана.
46. Петренко, С.А. Аудит безопасности Intranet [Электронный ресурс] : учебное пособие / С.А. Петренко, А.А. Петренко. - Электрон. дан. - Москва : ДМК Пресс, 2010. - 386 с. - Режим доступа: <https://e.lanbook.com/book/1113>. - Загл. с экрана.
47. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. - Электрон. дан. - Москва: ДМК Пресс, 2014. - 702 с. - Режим доступа: <https://e.lanbook.com/book/50578>. - Загл. с экрана.
48. Дудихин, В.В. Конкурентная разведка в Internet. Советы аналитика [Электронный ресурс]: учебное пособие / В.В. Дудихин, О.В. Дудихина. - Электрон. дан. - Москва: ДМК Пресс, 2009. - 192 с. - Режим доступа: <https://e.lanbook.com/book/1111>. - Загл. с экрана.
49. Семь безопасных информационных технологий [Электронный ресурс] : учебник / А.В. Барабанов [и др.] ; под ред. Маркова А.С.. - Электрон. дан. - Москва: ДМК Пресс, 2017. - 224 с. - Режим доступа: <https://e.lanbook.com/book/97352>. - Загл. с экрана.
50. Большат, Е.П. Проектирование комплексной системы защиты информации на предприятии (Конфиденциальная информация). [Электронный ресурс] - Электрон. дан. // Вестник научного общества студентов, аспирантов и молодых ученых. - 2015. - № 3. - С. 21-25. - Режим доступа: <http://e.lanbook.com/journal/issue/294140> - Загл. с экрана.
51. Зарубина, Л.П. Защита зданий, сооружений и конструкций от огня и шума. Материалы, технологии, инструменты и оборудование [Электронный ресурс]: учебное пособие / Л.П. Зарубина. - Электрон. дан. - Вологда: «Инфра-Инженерия», 2018. - 336 с. - Режим доступа: <https://e.lanbook.com/book/108662>. - Загл. с экрана.
52. Степанов-Егиянц, В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации [Электронный ресурс] : монография / В.Г. Степанов-Егиянц. - Электрон. дан. - Москва: СТАТУТ, 2016. - 190 с. - Режим доступа: <https://e.lanbook.com/book/92503>. - Загл. с экрана.

## **9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для прохождения практики, включая профессиональные базы данных и информационные справочные системы**

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при проведении практики:

1. <https://fstec.ru/> - сайт ФСТЭК России
2. <http://www.fsb.ru/> - сайт ФСБ РФ
3. <https://мвд.рф/> - сайт МВД РФ
4. <https://02.мвд.рф/> - сайт МВД по РБ
5. <http://www.consultant.ru/> - сайт Консультант Плюс
6. <http://www.bashlib.ru/echitzal/> - сайт ЭБС БашГУ
7. [http://biblioclub.ru/index.php?page=main\\_ub\\_red](http://biblioclub.ru/index.php?page=main_ub_red) - университетская библиотека онлайн
8. <https://e.lanbook.com/books> - ЭБС «Лань»
9. <https://www.securitylab.ru/> - сайт по ИБ
10. <https://www.anti-malware.ru/> - сайт по ИБ
11. <http://securitypolicy.ru/> - открытая библиотека документов по ИБ
12. <http://www.itsec.ru/> - Журнал информационная безопасность

Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем:

1. Справочная правовая система «Консультант Плюс» – <http://www.consultant-plus.ru>.
2. Электронная библиотечная система «Университетская библиотека онлайн» – <https://biblioclub.ru>.
3. Электронная библиотечная система издательства «Лань» – <https://e.lanbook.com/>
4. Электронный каталог Библиотеки БашГУ – <http://www.bashlib.ru/catalogi/>
5. <http://window.edu.ru/> – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
6. <http://univertv.ru/video/matematika/> – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
7. [www.newlibrary.ru](http://www.newlibrary.ru) – Новая электронная библиотека;
8. [www.edu.ru](http://www.edu.ru) – Федеральный портал российского образования;
9. [www.elibrary.ru](http://www.elibrary.ru) – Научная электронная библиотека;
10. [www.nehudlit.ru](http://www.nehudlit.ru) – Электронная библиотека учебных материалов.

## **10. Описание материально-технической базы, необходимой для проведения практики**

Место прохождения практики должно соответствовать действующим санитарно-эпидемиологическим требованиям, противопожарным правилам и нормам охраны здоровья обучающихся.

Место практики должно быть оснащено техническими и программными средствами, необходимыми для выполнения целей и задач практики: портативными и/или стационарными компьютерами с необходимым программным обеспечением и выходом в сеть Интернет, в том числе предоставляется возможность доступа к информации, размещенной в открытых и закрытых специализированных базах данных.

Конкретное материально-техническое обеспечение практики и права доступа студента к информационным ресурсам определяются руководителем конкретного студента, исходя из задания на практику.

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
<p><b>1. учебная аудитория для проведения групповых и индивидуальных консультаций:</b>  аудитория № 415 (гуманитарный корпус), аудитория № 416</p>	<p>Консультации</p>	<p><b>Аудитория № 415</b>  Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p><b>Аудитория № 416</b>  Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.</p> <p><b>Аудитория № 613</b>  Учебная мебель, доска, моноблок стационарный – 15 шт.</p>
<p>(гуманитарный корпус), <b>учебная аудитория для текущего контроля и промежуточной аттестации:</b>  аудитория № 415 (гуманитарный корпус), аудитория № 416</p> <p><b>2. помещения для самостоятельной работы:</b> аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).</p>	<p>Текущий контроль и промежуточная аттестация</p> <p>Самостоятельная работа</p>	<p><b>Аудитория 402 читальный зал библиотеки</b>  Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные</p> <ol style="list-style-type: none"> <li>Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.</li> <li>Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.</li> <li>Система централизованного тестирования БашГУ (Moodle). GNU General Public License. Лицензии бессрочные.</li> </ol>