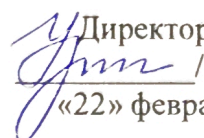


МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ
КАФЕДРА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

СОГЛАСОВАНО

на заседании Учебно-методической комиссии
института
Протокол № 7 от «22» февраля 2022 г.

УТВЕРЖДАЮ

 /А.И. Уразова
«22» февраля 2022 г.

ПРАКТИЧЕСКАЯ ПОДГОТОВКА
ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ
(ПРАКТИКИ ПО ПРОФИЛЮ СПЕЦИАЛИЗАЦИИ)

Б2.В.01.02(П)

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: 2022 г.

Уфа - 2022 г.

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

Программа утверждена на заседании ученого совета института, протокол № 6 от «24» февраля 2022 г.

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 в 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./

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, соотношенных с установленными в образовательной программе индикаторами достижения компетенций	5
3. Место практики в структуре образовательной программы	6
4. Объем практики.....	6
5. Содержание практики	6
6. Форма отчетности по практике.....	6
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике	7
8. Перечень учебной литературы и ресурсов сети Интернет, необходимых для проведения практики	14
9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для прохождения практики, включая профессиональные базы данных и информационные справочные системы	19
10. Описание материально-технической базы, необходимой для проведения практики	19

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

1.1. Вид и тип практики: производственная (практика по профилю специализации).

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 и 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 практики по профилю специальности является:

изучение организационной структуры производственного объекта по специальности, знакомство с его техническим оснащением, спецификой выполняемых работ, технологическими процессами, входящими в производственный цикл, получение навыков в определении информационных потоков на предприятии. Практика предполагает закрепление и дальнейшее развитие знаний, полученных при изучении теоретических курсов путем осмотра типичных средств защиты и систем информационной безопасности.

2.2. Основными задачами практики по профилю специальности являются:

- закрепление теоретических знаний, полученных в процессе обучения;
- приобретение информации, способствующей более глубокому усвоению теоретических курсов;
- изучение нормативной и технической документации выпускающей кафедры;
- получение практических навыков в области информационной безопасности;
- сформировать у студентов полное представление о своей будущей профессии.

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

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по практике
УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	ИУК-6.1	Знает основные способы оценки приоритетов
	ИУК-6.2	Умеет рационально прогнозировать распределение имеющихся ресурсов при постановки задач
	ИУК-6.3	Владеет навыками оценки ситуации и анализа приоритетов
ПК-3. Способен анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации	ИПК-3.1	Знает основные принципы и методы анализа защищенности компьютерных систем, проведения проверки 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
--	--	---

3. Место практики в структуре образовательной программы

Практика по профилю специальности 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 40 часов, в форме самостоятельной работы 176 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,	Результаты выполнения заданий
		описание работы подразделений предприятия, выработка предложений и рекомендаций по итогам прохождения практики	
3.	Заключительный этап	Обработка и анализ полученной информации, подготовка отчета по практике	Подборка материалов и документов, отчет по практике

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 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 соотношенных с ними запланированных результатов обучения по практике. Описание критериев и шкал оценивания результатов обучения по практике.

УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни

Код и наименование индикатора достижения компетенции	Результаты обучения по практике	Критерии оценивания	Шкала оценивания
ИУК-6.1	Знает основные способы оценки приоритетов	Знает основные способы оценки приоритетов	отлично
		В целом знает основные способы оценки приоритетов	хорошо
		Имеет фрагментарные знания об основных способах оценки приоритетов	удовлетворительно
		Знает основные способы оценки приоритетов	неудовлетворительно

ИУК-6.2	Умеет рационально прогнозировать распределение имеющихся ресурсов при постановки задач	Умеет рационально прогнозировать распределение имеющихся ресурсов при постановки задач	отлично
		В целом умеет рационально прогнозировать распределение имеющихся ресурсов при постановки задач, но допускает незначительные ошибки	хорошо
		Умеет рационально прогнозировать распределение имеющихся ресурсов при постановки задач, но допускает значительные ошибки	удовлетворительно
		Не умеет рационально прогнозировать распределение имеющихся ресурсов при постановки задач	неудовлетворительно
ИУК-6.3	Владеет навыками оценки ситуации и анализа приоритетов	Владеет навыками оценки ситуации и анализа приоритетов	отлично
		Уверенно владеет навыками оценки ситуации и анализа приоритетов, но допускает незначительные ошибки	хорошо
		Владеет навыками оценки ситуации и анализа приоритетов, но допускает значительные	удовлетворительно

		ошибки	
		Не владеет навыками оценки ситуации и анализа приоритетов	неудовлетворительно

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

Код и наименование индикатора достижения компетенции	Результаты обучения по практике	Критерии оценивания	Шкала оценивания
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

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

		проверки работоспособности и эффективности применяемых средств защиты информации, но допускает незначительные ошибки	
		Владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации, но допускает значительные ошибки	удовлетворительно
		Не владеет использованием основных принципов и методов анализа защищенности компьютерных систем, проведения проверки работоспособности и эффективности применяемых средств защиты информации	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. Изучение политики безопасности для защиты системы отбора персонала предприятия.
2. Изучение системы информационной безопасности для ЛВС предприятия.
3. Исследование технико-экономических характеристик аппаратно-программных средств для блокировки мобильной связи.
4. Изучение системы видеонаблюдения для платежного терминала.
5. Разработка метода защиты вычислительной системы.
6. Разработка программного обеспечения для мониторинга доступа к пакету услуг на платформе ОС WindowsXP/7
7. Проектирование микропроцессорной системы охранной сигнализации.
8. Разработка метода восстановления данных с поврежденных носителей информации.
9. Исследование технико-экономических характеристик аппаратно-программных средств для блокировки мобильной связи.
10. Модернизация системы информационной безопасности для предприятия.

Примерные вопросы к зачету:

11. Каковы назначение, цели деятельности, структура учреждения (предприятие, организация), в которой проходила практика?
12. На основании каких учредительных документов функционирует данное учреждение (предприятие, организация)?
13. Какими основными нормативно-правовыми актами руководствуется в своей деятельности данное учреждение (предприятие, организация)?
14. Какие знания, умения и навыки были приобретены или развиты в результате прохождения практики?
15. Какие задания были выполнены в ходе прохождения практики?
16. Какие документы (проекты документов) были составлены?

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 и 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. Собурь, С.В. Установки пожарной сигнализации / С.В. Собурь. - 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. Собурь, С.В. Пожарная безопасность электроустановок / С.В. Собурь. - 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. Кувыклин, 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. Зефилов, 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

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. Больбат, 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.

19. 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.

20. 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 - 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 – Новая электронная библиотека;
8. www.edu.ru – Федеральный портал российского образования;
9. www.elibrary.ru – Научная электронная библиотека;
10. 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>1. учебная аудитория для проведения групповых и индивидуальных консультаций: аудитория № 415 (гуманитарный корпус), аудитория № 416</p>	<p>Консультации</p>	<p>Аудитория № 415 Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт APART MA1225 – 1 шт.</p> <p>Аудитория № 416 Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinop – 1 шт.</p> <p>Аудитория № 613 Учебная мебель, доска, моноблок стационарный – 15 шт.</p>
<p>(гуманитарный корпус), учебная аудитория для текущего контроля и промежуточной аттестации: аудитория № 415 (гуманитарный корпус), аудитория № 416 2. помещения для самостоятельной работы: аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).</p>	<p>Текущий контроль и промежуточная аттестация</p> <p>Самостоятельная работа</p>	<p>Аудитория 402 читальный зал библиотеки Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные</p> <p>1. 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.</p> <p>2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.</p> <p>3. Система централизованного тестирования БашГУ (Moodle). GNU General Public License. Лицензии бессрочные.</p>