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

Утверждено:
на заседании кафедры
протокол № 9 от 24.04.2020
Зав. кафедрой / А.С. Исмагилова

Согласовано:
Председатель УМК института
/ Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Международные и российские акты и стандарты по информационной безопасности
Б1.В.1.04 (вариативная)

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации

Квалификация
Бакалавр

Разработчик:
к.филос.н.
старший преподаватель кафедры
/ Миронова Н.Г.
/ Оводов А.М.

Для приема: 2020 г.

Уфа 2020 г.

Составители: Н.Г.Миронова, А.М. Оводов

Рабочая программа дисциплины утверждена на заседании кафедры управления информационной безопасностью от 24.04.2020 № 9

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры управления информационной безопасностью, протокол № __ от «__» _____ 20__ г.

Заведующий кафедрой _____/ _____Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с результатами освоения образовательной программы

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	Знать основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ Знать основные понятия, цели, принципы, сферы применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, роль договоров в сфере информационной безопасности; виды юридической ответственности Знать методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	**ОПК-5:** способность использовать нормативные правовые акты в профессиональной деятельности	
	Знать нормативные документы для обоснования безопасности конфиденциальной информации в информационных системах, на объектах информатизации, информационно- аналитического и информационно-психологического обеспечения правоохранительной деятельности	**ПК-9**: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации Знать общеметодологические принципы теории информационной безопасности Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации Знать состояние законодательной базы и стандарты в области информационной безопасности	**ПК-13:** способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
Умения	Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности; Уметь предвидеть юридические опасности и угрозы, связанные с использованием информации, и соблюдать основные правовые требования информационной безопасности, в т.ч. защиты интеллектуальной собственности; предпринимать необходимые меры по восстановлению нарушенных прав	**ОПК-5:** способность использовать нормативные правовые акты в профессиональной деятельности	
	Уметь собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности по вопросам обеспечения безопасности информации на объектах информатизации, информационно- аналитическо-	**ПК-9**: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обес-	

	го и информационно-психологического обеспечения правоохранительной деятельности	печения информационной безопасности по профилю своей профессиональной деятельности	
	Уметь реализовывать на практике принципы политики безопасности; Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности Уметь обосновывать организационно-технические мероприятия по защите информации Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	**ПК-13:** способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
Навыки, опыт деятельности	Владеть навыками анализа юридических последствий, связанных с использованием информации Владеть опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	**ОПК-5:** способность использовать нормативные правовые акты в профессиональной деятельности	
	Владеть навыками сбора и обработки необходимых данных; навыками анализа и интерпретации содержащейся в различных источниках информации, на объектах информатизации, информационно- аналитического и информационно-психологического обеспечения правоохранительной деятельности	**ПК-9**: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	
	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации Владеть навыками выявления и устранения угроз информационной безопасности Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий Владеть навыками внедрения, адаптации и настройки средств защиты прикладных ИС	**ПК-13:** способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Международные и российские акты и стандарты по информационной безопасности» относится к вариативной части образовательной программы.

Дисциплина «Международные и российские акты и стандарты по информационной безопасности» изучается на 3-м курсе в 5 семестре.

Цели изучения дисциплины: усвоение международной и отечественной нормативно-правовой базы, стандартов и требований сертификации в области обеспечения информационной безопасности.

Для освоения дисциплины «Международные и российские акты и стандарты по информационной безопасности» необходимы знания и компетенции ОПК-5; ПК-9; ПК-13, сформирован-

ные в рамках изучения следующих дисциплин и видов практики: Основы информационной безопасности, Программно-аппаратные средства защиты информации, Организационное и правовое обеспечение информационной безопасности, Правоведение, Организационное и правовое обеспечение информационной безопасности, Документоведение, Правовая охрана результатов интеллектуальной деятельности, а также практика по получению первичных профессиональных умений, практика по получению профессиональных умений и опыта профессиональной деятельности.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап	Знать основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ Знать основные понятия, цели, принципы, сферы применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, роль договоров в сфере информационной безопасности; виды юридической ответственности Знать методы и средства правовой защиты интересов	Не знает, не знает иностранной терминологии в области ИБ	Демонстрирует целостные, системные знания, терминологию в указанной сфере, свободно ориентируется в них при решении практических задач.

	субъектов в сфере информационной безопасности		
Второй этап	Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности; Уметь предвидеть юридические опасности и угрозы, связанные с использованием информации, и соблюдать основные правовые требования информационной безопасности, в т.ч. защиты интеллектуальной собственности; предпринимать необходимые меры по восстановлению нарушенных прав	Не способен освоить материал или ресурс, если он на иностранном языке	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации
Третий этап	Владеть навыками анализа юридических последствий, связанных с использованием информации Владеть опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	Не владеет навыком при необходимости освоить материал или ресурс на иностранном языке	Демонстрирует уверенное, свободное владение иностранным языком при решении профессиональных задач.

ПК-9: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

Этап (уровень) освоения компе-	Планируемые результаты обучения (показатели достижения заданного уровня освое-	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»

тенции	ния компетенций)		
Первый этап	Знать нормативные документы для обоснования безопасности конфиденциальной информации в информационных системах, на объектах информатизации, информационно- аналитического и информационно-психологического обеспечения правоохранительной деятельности	Не демонстрирует указанных знаний	Демонстрирует целостные, системные знания в указанной сфере, свободно ориентируется в них при решении практических задач.
Второй этап	Уметь собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности по вопросам обеспечения безопасности информации на объектах информатизации, информационно- аналитического и информационно-психологического обеспечения правоохранительной деятельности	Не умеет	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации
Третий этап	Владеть навыками сбора и обработки необходимых данных; навыками анализа и интерпретации содержащейся в различных источниках информации, на объектах информатизации, информационно- аналитического и информационно-психологического обеспечения правоохранительной деятельности	Не владеет и не имеет теоретических знаний об этой сфере	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации.

ПК-13: способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»

Первый этап	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации Знать общеметодологические принципы теории информационной безопасности Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации Знать состояние законодательной базы и стандарты в области информационной безопасности	Не демонстрирует указанных знаний	Демонстрирует целостные, системные знания в указанной сфере, свободно ориентируется в них при решении практических задач.
Второй этап	Уметь реализовывать на практике принципы политики безопасности; Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности Уметь обосновывать организационно-технические мероприятия по защите информации Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	Не умеет	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации
Третий этап	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью Владеть навыками организации комплекса	Не владеет и не имеет теоретических знаний об этой сфере	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации.

	мероприятий по защите информации в процессах автоматизированной обработки информации Владеть навыками выявления и устранения угроз информационной безопасности Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий Владеть навыками внедрения, адаптации и настройки средств защиты прикладных ИС		

4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1-й этап Знания	Знать основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ Знать основные понятия, цели, принципы, сферы применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, роль договоров в сфере информационной безопасности; виды юридической ответственности Знать методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	**ОПК-5:** способность использовать нормативные правовые акты в профессиональной деятельности	опрос
	Знать нормативные документы для обоснования безопасности конфиденциальной информации в информационных системах, на объектах информатизации, информационно- аналитического и информационно-психологического обеспечения правоохранительной деятельности	**ПК-9**: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Опрос, практические задания, коллоквиум, тесты, зачет
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	**ПК-13:** способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по	Опрос, практические задания, коллоквиум, тесты,

	Знать общеметодологические принципы теории информационной безопасности Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации Знать состояние законодательной базы и стандарты в области информационной безопасности	обеспечению информационной безопасности, управлять процессом их реализации	зачет
2-й этап Умения	Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности; Уметь предвидеть юридические опасности и угрозы, связанные с использованием информации, и соблюдать основные правовые требования информационной безопасности, в т.ч. защиты интеллектуальной собственности; предпринимать необходимые меры по восстановлению нарушенных прав	**ОПК-5:** способность использовать нормативные правовые акты в профессиональной деятельности	Опрос, практические задания, коллоквиум, тесты, зачет
	Уметь собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности по вопросам обеспечения безопасности информации на объектах информатизации, информационно- аналитического и информационно-психологического обеспечения правоохранительной деятельности	**ПК-9**: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Опрос, практические задания, коллоквиум, тесты, зачет
	Уметь реализовывать на практике принципы политики безопасности; Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности Уметь обосновывать организационно-технические мероприятия по защите информации Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	**ПК-13:** способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Опрос, практические задания, коллоквиум, тесты, зачет
3 этап - владения, навыки	Владеть навыками анализа юридических последствий, связанных с использованием информации Владеть опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	**ОПК-5:** способность использовать нормативные правовые акты в профессиональной деятельности	Опрос, практические задания, коллоквиум, тесты, зачет
	Владеть навыками сбора и обработки необходимых данных; навыками анализа и интерпретации содержащейся в различных источниках информации, на объектах информатизации, информационно- аналитического и информационно-психологического обеспечения правоох-	**ПК-9**: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной	Опрос, практические задания, коллоквиум, тесты, зачет

	ранительной деятельности	безопасности по профилю своей профессиональной деятельности	
	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации Владеть навыками выявления и устранения угроз информационной безопасности Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий Владеть навыками внедрения, адаптации и настройки средств защиты прикладных ИС	**ПК-13:** способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Опрос, практические задания, коллоквиум, тесты, зачет

4.3. Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 2.

Типовые темы практических и лабораторных занятий

Модуль 1. Международная и национальная нормативно-правовая база в области обеспечения информационной безопасности

1.1 Законодательство РФ в области информационной безопасности.
1.2 Правовые основы защиты информации, коммерческой и государственной тайны. **Тест 1**.
1.3 Изучение положений о государственном лицензировании деятельности в области защиты информации. **Тест 2.**
1.4 Анализ сертификата соответствия.
1.5 Изучение положений о сертификации средств защиты информации по требованиям безопасности информации.
1.6 Система сертификации средств криптографической защиты информации. **Тест 3.** «Отечественные нормативные документы в области криптографической защиты»

Модуль 2. Международные и национальные стандарты по информационной безопасности

2.1. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации.
2.2. Изучение особенностей аттестации помещений по требованиям безопасности информации. **Итоговое тестирование.**

Типовые вопросы для семинаров

Устный индивидуальный опрос/доклад проводится после изучения новой темы, во время практического занятия, с целью выяснения сложных вопросов, для оценки степени усвоения материалов, компетенций. Студент излагает содержание вопроса изученной темы в виде устного доклада либо отвечает на поставленный устный вопрос по теме из нижеприведенного списка, предварительно ознакомившись с материалами лекции и дополнительной литературы.

Модуль 1. Международная и национальная нормативно-правовая база в области обеспечения информационной безопасности

Тема 1.1. Законодательство РФ в области информационной безопасности.

1. Конституция РФ, федеральные законы и кодексы в области защиты информации;
2. Указы Президента РФ, постановления Правительства РФ об информационной безопасности;
3. Международная нормативно-правовая база в области обеспечения информационной безопасности.
4. Нормативно-правовая база Федеральной службы по техническому и экспортному контролю (ФСТЭК) России по информационной безопасности;
5. Нормативно-правовая база ФСБ, других Министерств, ведомств и служб РФ в области защиты информации (МО РФ, ФСО России, МВД РФ, Минкомсвязи РФ, Роскомнадзора и др.
6. Основные законы в области информационной безопасности.
7. Источники правовой информации.
8. Устный опрос, практическое задание.

Тема 1.2. Правовые основы защиты информации, коммерческой и государственной тайны. Тест 1.

1. Понятие конфиденциальной информации. Виды тайны. Коммерческая тайна.
2. Государственная тайна, ее виды, нормативные акты, регулирующие работы с информацией, представляющей гостайну.
3. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности.
4. Использование грифов секретности.
5. Правовые режимы защиты информации.
6. **Тестирование (1 час) – тест 1.**

Тема 1.3. Изучение положений о государственном лицензировании деятельности в области защиты информации. Тест 2.

1. Руководящие документы ФСТЭК по сертификации и лицензированию в области ЗИ.
2. Закон о «О техническом регулировании»
3. Закон о «О лицензировании отдельных видов деятельности»
4. Функции государственных органов и лицензионных центров по лицензированию в области защиты информации.
5. Сертификация в области защиты информации (обязательная и добровольная).
6. Порядок проведения лицензирования и контроля за деятельностью лицензиатов.
7. Устный опрос, практическое задание.

Тема 1.4. Анализ сертификата соответствия

1. Особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах.

2. Маркировка сертифицированной продукции.
3. Сертификат соответствия (надо описать содержание и внешний вид сертификата соответствия).
4. Признаки СС, указывающие на подлинность или недействительность сертификата соответствия.
5. Устный опрос, практическое задание.
6. **Тестирование: Тест 2.**

Тема 1.5. Изучение положений о сертификации средств защиты информации по требованиям безопасности информации.

1. Требования по защите персональных данных.
2. Способы поиска информации в справочно-правовых системах.
3. Поиск нормативных документов в области сертификации с помощью информационно-поисковых системы.
4. Информация о сертификации на сайте ФСТЭК (практическое знакомство с выполнение конкретных заданий).
5. Устный опрос, практическое задание.

Тема 1.6. Система сертификации средств криптографической защиты информации.

1. Особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами.
2. Лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.
3. Классификация программных и технических средств, сертифицируемых для работы с конфиденциальной информацией (классы ПО, ОС, ИС, АСУ и т.д.).
4. Устный опрос, практическое задание.
5. **Тестирование** (Тест 3). «Отечественные нормативные документы в области криптографической защиты»

Модуль 2. Международные и национальные стандарты по информационной безопасности

Тема 2.1. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации.

1. Зарубежные/международные стандарты в области защиты информационных систем.
2. Адаптированные международные стандарты в виде национальных ГОСТов в области ЗИ.
3. Стандарт ISO/IEC 27001:2005
4. Устный опрос, практическое задание.
5. Коллоквиум по индивидуальным темам.

Тема 2.2. Изучение особенностей аттестации помещений по требованиям безопасности информации.

1. Устный опрос, практическое задание.
2. Аттестация помещений по требованиям безопасности информации – выполнение задания
3. Устный опрос, практическое задание.
4. Выполнение практического задания.
5. Итоговое тестирование.

Критерии и методика оценивания (в баллах):

Количество докладов и заданий для 1 студента в течение изучения курса – до 10 (включительно), «ценой» от 0 до 1 балла за каждый ответ на 1 вопрос
- 1 балл – если студент дает неполный или недостаточно актуальный по содержанию ответ в докладе,
- 2 балла – если студент дает полный и правильный ответ в докладе.

Типовые вопросы устных опросов и практических заданий

По сложности задания разделяются на простые и комплексные задания.

Простые задания (уровень I) предполагают ответ на вопрос (уровень компетенции - знать) или решение (уровень компетентности – уметь, владеть навыком). К простым заданиям можно отнести: простые ситуационные задачи с коротким ответом или простым действием; несложные задания по выполнению конкретных действий. Простые задания применяются для оценки знаний и умений.

Комплексные задания (уровень II) требуют многоходовых решений как в типичной, так и в нестандартной ситуациях. Это задания в открытой форме, требующие поэтапного решения и развернутого ответа, в т.ч. задания на индивидуальное или коллективное выполнение проектов, на выполнение практических действий или лабораторных работ. Комплексные практические задания применяются для оценки владений.

Примерные формулировки практических контрольных заданий I- простые, II - комплексные задания; знать – «З», уметь – «У», владеть – «В»

Примерные вопросы для проверки знаний по компетенции ОПК-3:

ОПК-11 – I.В

В сети Интернет:

- Найти документы, в т.ч. международные, в которых обязательно присутствует слово «юридическая» и обязательно отсутствует слово «деятельность». Использовать соответствующие операторы.
- Найти нормативные документы в области стандартизации деятельности в области защиты информации (в т.ч. международные), которые содержат слово «маркетинг» или «производство», но не содержат слово «реклама» (подсказка: используйте при поиске поисковые операторы браузеров, исключающие слова из поисковой выдачи).
- Найти термины «юридическая деятельность» на сайте БашГУ (использовать оператор поиска на определенном сайте).

и т.д.

Примерные вопросы для проверки знаний по компетенции ПК-9:

ПК-9 – I.З

- К какому виду информации относится записанный на бумаге текст программы для ЭВМ?
- Дайте корректное определение термину «защищаемое помещение» (в контексте ИБ)? В каком нормативе дается определение этого термина?
- Кому подведомственен ФСТЭК России?

ПК-9 – II.З

Классифицируйте АС. В АС работают: один пользователь, один администратор ИБ. В АС хранится информация одного уровня конфиденциальности. Насчет разграничения прав доступа (разные/ равные права): права определенно разные т.к. у администратора ИБ должен быть полный доступ ко всей информации, обычным пользователям полный доступ не предоставлен.

ПК-9 – I.У

Определение требований к защите и категорирование ресурсов.

ПК-9 – I.У

Поиск информации на заданную тему в рецензируемых журналах в области информационной безопасности.

ПК-9 – II.У

Организация собирается аттестовать саму себя под 1Г. СТР-К требует, чтобы закрытые АС не подключались к интернету, даже через МЭ, но интернет нужен бухгалтерии, компьютеры которой предполагается так же аттестовать. Что можно сделать в этой ситуации?

ПК-9 – II.У

Классы защищенности согласно «Оранжевой книге»

ПК-9 – I.В

Сравнение основных справочно-правовых систем.

ПК-9 – II.В

Написание доклада на тему «Современные средства антивирусной защиты»

Примерные вопросы для проверки знаний по компетенции ПК-19:

ПК-13 – I.З

- Порядок проведения аттестации ИС и ИСПДн.
- Каким нормативным актом/постановлением описывается порядок определения уровней защищённости персональных данных?

ПК-13 – II.У

Нужно аттестовать программное или техническое средство защиты для получения лицензии по ТЗКИ с минимальными затратами. Какой порядок/алгоритм действия, в соответствии с отечественной законодательной базой?

ПК-13 – II.У

Как проводится обследование подсистем / инвентаризация / категорирование / документирование защищаемых ресурсов автоматизированных систем?

ПК-13 – I.В

Как провести испытания объектов на соответствие организационно-техническим требованиям по защите информации.

ПК-13 – II.В

Получение лицензии на деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах.

ПК-13 – II.В

Нужно провести испытание объекта защиты на соответствие требованиям по защите информации от утечки за счет ПЭМИН средств вычислительной техники (СВТ). Каков алгоритм действий, в соответствии с отечественной нормативной базой и сложившейся практикой?

ПК-13 – II.В

Найдите информацию о СЗИ (в т.ч. международных нормативных актов), достаточных для построения защиты АС класса защищенности 1Д.

Критерии и методика оценивания результата устного опроса. Студент может быть опрошен неоднократно в течении разных практических занятий, за каждый ответ на 1 из вышеприведенных вопросов по проверке усвоения компетенции может начислено до 1 балла за правильный ответ.

Критерии и методика оценивания качества выполнения заданий практических занятий:
- 2 балла выставляется студенту, если практическое задание выполнено без ошибок и полно;
- 1 балл – если ответ на вопрос дан верно и достаточно полно или поставленная цель при решении задачи достигнута частично (на 30-70%).
- 0 баллов выставляется студенту, если работа не выполнена или выполнена менее, чем на 50%, (либо ответ на устный вопрос не дан или дан неверно).

Типовые тестовые задания

При изучении дисциплины используются 4 теста (3 теста в Модуле 1, 1 тест – в Модуле 2); тестовые задания – открытого и закрытого типа. Каждое тестовое задание включает вопрос и несколько вариантов ответов к нему либо предполагает вписывание правильного словосочетания, термина, даты и т.п. в текст тестового вопроса. Тестирование выполняется в письменной форме или в виде on-line-тестирования (в системе Moodle, http://moodle.bashedu.ru/) во время практических занятий по результату изучения теоретического материала. Критерии оценки каждого теста различны (баллы за тесты приводятся в конце каждого теста ниже).

Модуль 1. Международная и национальная нормативно-правовая база в области обеспечения информационной безопасности

Тест 1. «Правовое нормативное регулирование деятельности в области информационной безопасности и защиты информации РФ»

Внесите информацию в пустые поля (заполните пропуски данными, словами или фразами):

1. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О _____ отдельных видов деятельности».
2. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об _____подписи».
3. Федеральный закон от 28 декабря 2010 г. № _____ФЗ «О безопасности».
4. Федеральный закон от 27 июля _____г. № 152-ФЗ «О персональных данных».
5. Федеральный закон от 27 июля _____г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Критерий оценивания Теста № 1: 30 вопросов – до 9 баллов (1 правильно сделанный вопрос теста = 0,3 балла)

Тест 2. Нормативная международная и отечественная база по защите информации

Внесите информацию в пустые поля в названиях нормативных документов:.
1. «_____ требования и рекомендации по технической защите конфиденциальной информации» (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
2. «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по _____ каналам». Гостехкомиссия России. - М., 2002.
3. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические _____. Госстандарт России. - М., 1995.
4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие _____. Госстандарт России. - М., 2006.
5. ГОСТ Р 50922-2006. Защита информации. Основные термины и _____. - М., 2006.

и т.д.

Критерий оценивания Теста № 2: 40 вопросов – до 12 баллов (1 правильно сделанный вопрос теста = 0,3 балла)

Тест 3. Отечественные нормативные документы в области криптографической защиты

1. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № ____ «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».
2. Приказ ФСБ России от _____ июля _____ г. № _____ «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
3. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки _____ . Защита криптографическая. Алгоритм криптографического преобразования.
4. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. _____ защита информации. Процессы формирования и проверки электронной цифровой подписи.
5. ГОСТ Р 34.10-_____ Государственный стандарт Российской Федерации. Информационная технология. _____ защита информации. Процессы формирования и проверки электронной цифровой подписи.

   и т.д.

Критерий оценивания Теста № 3: 10 вопросов – до 4 баллов (1 правильно сделанный вопрос теста = 0,4 балла)

Модуль 2. Международные и национальные стандарты по информационной безопасности

Итоговый тест № 4

1 Уровень безопасности С, согласно "Оранжевой книге", характеризуется:

а. произвольным управлением доступом
б. принудительным управлением доступом
в. верифицируемой безопасностью

2. Согласно стандарту X.700, в число функций управления безопасностью входят:

а. создание инцидентов
б. реагирование на инциденты
в. устранение инцидентов

3. Согласно рекомендациям X.800, выделяются следующие сервисы безопасности:

а. аутентификация
б. идентификация
в. туннелирование

4 Т.н. стандарт информационной безопасности «Общие критерии» содержит следующие виды требований:
а. функциональные
б. доверия безопасности
в. экономической целесообразности

5. В число классов функциональных требований "Общих критериев" входят:
а. анонимность
б. приватность
в. связь

и т.д.

Критерий оценивания Теста № 4: 20 вопросов – до 5 баллов (1 правильно сделанный вопрос теста = 0,25 балла).

Подробнее тесты приведены в ФОС.

Методические указания по выполнению Контрольной самостоятельной работы

Для предприятия, выбранного согласно вашему варианту (вариант определяется по последней цифре зачетной книжки студента), следует составить список нормативных правовых актов и стандартов, которыми необходимо руководствоваться при построении комплексной системы защиты информации предприятия. К каждому документу представить комментарий, указывающий обязательный или рекомендательный характер документа, основное содержание документа, область применения документа для рассматриваемого вами предприятия.

Примерные варианты тем самостоятельной контрольной работы (КСР)

1. факультет университета;
2. филиал банка;
3. небольшое торговое предприятие;
4. поликлиника;
5. больница;
6. железнодорожная станция;
7. школа;
8. библиотека;
9. юридическая фирма;
10. фирма по разработке программного обеспечения.

Отчет оформите с титульным листом по принятым в России ГОСТам оформления научно-исследовательских работ, с указанием вуза, кафедры, специальности, дисциплины, варианта, года и т.д. Приложите Оглавление (2-й лист отчета), Введение (с постановкой задач и описанием заданий), Вывод и Список использованных источников.

Отчет должен быть зарегистрирован в учебной части и сдан для проверки преподавателю на кафедру управления информационной безопасности (к. 417) за несколько недель или дней до сессии.

Критерии и методика оценивания самостоятельной контрольной работы:

- **5 баллов** студент получает, если работа выполнена в полном объеме и изложена грамотным языком в правильной логической последовательности с точным использованием специализированной терминологии; если при этом показано уверенное владение прикладными программами.
- **4 балла** студент получает за самостоятельную контрольную работу, если она выполнена в полном объеме, но имеет один из недостатков:
  - в работе допущены один-два недочета при освещении основного содержания ответа;
  - нет определенной логической последовательности, неточно используется специализированная терминология;
- **3 балла и менее** студент получает, если работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков (пропорционально количеству недочетов, ошибок, пробелов в знаниях).

Оценочные баллы выставляются по результату защиты КСР на предпоследнем практическом занятии.

Типовые материалы для самоконтроля

1. Конституция РФ, федеральные законы и кодексы в области защиты информации.
2. Указы Президента РФ, постановления Правительства РФ об информационной безопасности.
3. Международная нормативно-правовая база в области обеспечения информационной безопасности.
4. Нормативно-правовая база Федеральной службы по техническому и экспортному контролю (ФСТЭК) России по информационной безопасности.
5. Нормативно-правовая база ФСБ, других Министерств, ведомств и служб РФ в области защиты информации (МО РФ, ФСО России, МВД РФ, Минкомсвязи РФ, Роскомнадзора и др.
6. Стандарт Центробанка России от 01.06.2014 г. «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения» (СТО БР ИББС-1.0–2014)
7. Использование грифов секретности.
8. Окинавская «Хартия глобального информационного общества»;
9. Директива по безопасности информационных систем и сетей ОЭСР 2002 г. «К культуре безопасности» ОЭСР и принципы операционного риска Банка международных расчетов(Basel II).
10. Стандарты ISO/IEC 17799:2005, ISO/IEC 27000, ISO/IEC 27001:2005, ISO/IEC 27002, ISO/IEC 27005;
11. Стандарты DOD , TCSEC (оранжевая книга) США, GreenBook Германия, WhiteBook (ITSEC).
12. Закон о «О техническом регулировании»
13. Сертификация в области защиты информации (обязательная и добровольная).
14. Закон о «О лицензировании отдельных видов деятельности»
15. Функции государственных органов и лицензионных центров по лицензированию в области защиты информации.
16. Порядок проведения лицензирования и контроля за деятельностью лицензиатов.
17. Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
18. Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?
19. Назовите лицензионные требования и условия при осуществлениидеятельности по техническому обслуживанию шифровальных (криптографических) средств.
20. Сертификат соответствия. Опишите документ. Какие признаки в СС указывают на его подлинность или недействительность.

21. Маркировка сертифицированной продукции.
22. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации. Функции органов сертификации, испытательных лабораторий, ФСТЭК.
23. Назовите виды и схемы сертификации средств защиты информации.
24. Общий порядок проведения сертификации средств защиты информации.
25. Сертификат соответствия. Какие признаки в СС указывают на его подлинность или недействительность Маркировка сертифицированной продукции
26. Организационная структура системы сертификации технических, программно-технических, программных автоматизированных систем и локальных вычислительных сетей на соответствие требованиям по безопасности информации.
27. РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»
28. Классы защищенности АС от НСД к информации. Требования по защите информации от НСД для АС.
29. Классы защищенности СВТ и МЭ. Показатели защищенности СВТ;
30. СТР-К
31. Национальные стандарты РФ ГОСТ-ИСО/МЭК по информационной безопасности;
32. ГОСТ Р ИСО/МЭК 15408-2002. Профиль защиты и задание по безопасности.
33. ГОСТ Р ИСО/МЭК 15408-2002. Функциональные требования безопасности.
34. ГОСТ Р ИСО/МЭК 15408-2002. Оценочные уровни доверия.
35. ГОСТ Р ИСО/МЭК 15408-2002. Область применения документа, краткий обзор.
36. Приказы ФСТЭК России (N 17, N 489, N 21 и т.д.)
37. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
38. Аттестация ИС и ИСПДн.

Критерии оценки результатов собеседования (в баллах):

- 15 баллов выставляется, если студент демонстрирует глубокое или обширное владение материалом, уверенно излагает материал и отвечает на вопросы по основной теме.
- 6-14 баллов – если студент знает тему фрагментарно или допускает ошибки в изложении материала и или логике изложения и выводах.
- 1-6 баллов, если студент слабо осведомлен в теме и/или не может дать содержательного ответа на дополнительные вопросы по теме.

Зачет

Форма итого контроля по дисциплине Информационные технологии – зачет; зачет выставляется по результатам текущего и рубежного контроля успеваемости студента. Критерии оценки (в баллах):

- «Зачтено» выставляется студенту, если он набрал по результатам изучения дисциплины 60 баллов;
- «Не зачтено» выставляется студенту, если он набрал менее 59 баллов.

Максимальная сумма баллов с учетом форм текущего и рубежного контроля может составлять 100 баллов.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная учебная литература:

1. Правовое обеспечение информационной безопасности: Учебное пособие. - М.: Маросейка, 2008. – 368 с. http://biblioclub.ru/index.php?page=book&id=96249&sr=1
2. Загинайлов Ю.Н.Теория информационной безопасности и методология защиты информации: учебное пособие. - М., Берлин: Директ-Медиа, 2015. – 253 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557&sr=1

б) дополнительная учебная литература:

3. Аверченков В.И., Рытов М.Ю. Организационная защита информации: учебное пособие для вузов. - М.: Флинта, 2011. – 184 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=93343&sr=1
4. Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р. Защита персональных данных в организации. - М.: Флинта, 2011. – 124 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=93260&sr=1

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1. Справочная правовая система «КонсультантПлюс» – 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. www.fstec.ru –сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. 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);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. 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.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
1. *учебная аудитория для проведения занятий лекционного типа:* аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2. *учебная аудитория для проведения лабораторных работ*:** Лаборатория полигон технической защиты информации № 508 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (гуманитарный корпус). **3. *учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **4. *учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гу-	Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 415** 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. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard	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. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License..

манитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **5.** ***учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **6.** ***помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **7.*помещение для хранения и профилактического обслуживания учебного оборудования:*** аудитория № 523 (гуманитарный корпус).		387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру INTEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Лаборатория полигон технической защиты информации № 508** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технической защиты информации, комплекс мониторинга WiFi сетей "Зодиак II", универсальный ком-плект инструментов для проведения работ по специальным провер-кам и специальным обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон". **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.	

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Содержание рабочей программы
дисциплины «Международные и российские акты и стандарты по информационной безопасности»
на 5 семестр ОФО

Вид работы	Объем дисциплины
	ОФО
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 ЗЕТ / 72 часа
Учебных часов на контактную работу с преподавателем:	36,2
лекций	18
практических/ семинарских	8
лабораторных	10
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	35,8
Учебных часов на подготовку к экзамену (Контроль)	

Форма контроля
Зачет 5 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР	ЛР	СРС			
1	2	4	5	6	7	8	9	10
	Модуль 1. Международная и национальная нормативно-правовая база в области обеспечения информационной безопасности							
1	1.1 Международная нормативно-правовая база в области обеспечения информационной безопасности. **Содержание:** Окинавская «Хартия глобального информационного общества»; международные организации и нормативные акты безопасности. Директива по безопасности информационных систем и сетей ОЭСР 2002 г. «К культуре безопасности» ОЭСР и принципы операционного риска Банка международных расчетов (Basel II).	2	2	1	7	1-2	Самост. изучение источников и материалов, выполнение домашнего и аудиторного практических заданий, подготовка к семинарам и тесту.	Т, ПЗ, КР, К
2	1.2 Национальная нормативная база РФ в области информационной безопасности **Содержание:** Структура и состав информационного законодательства РФ. Международные договоры РФ, Конституция РФ, федеральные законы и кодексы в области информационной безопасности. Указы Президента РФ, постановления Правительства РФ об информационной безопасности. Нормативно-правовая база Федеральной службы по техническому и экспортному контролю (ФСТЭК) России по информационной безопасности. Нормативно-правовая база ФСБ, других Министерств, ведомств и служб РФ в области защиты информации (МО РФ, ФСО России, МВД РФ,	4	2	1	8	1-3	Самостоятельное изучение рекомендуемых источников и материалов, подготовка к семинарскому занятию.	Т, ПЗ, КР, К

	Минкомсвязи РФ, Роскомнадзора и др.).							
3	1.3. Общие сведения о стандартизации, сертификации и метрологии **Содержание:** Основы стандартизации и метрологии в ИБ, сертификация в области защиты информации.	2	2	2	7	1-3	Самостоятельное изучение рекомендуемых источников и материалов, подготовка к семинарскому занятию.	Т, ПЗ, КР,
Модуль 2. Международные и национальные стандарты по информационной безопасности								
4	2.1. Международные стандарты по информационной безопасности. **Содержание**. Стандарты BS 7799-1:2005, BS 7799-2:2005, BS 7799-3:2006 (построения СУИБ). Стандарты ISO/IEC 17799:2005, ISO/IEC 27000, ISO/IEC 27001:2005, ISO/IEC 27002, ISO/IEC 27005. DOD, TCSEC (оранжевая книга) США, GreenBook Германия, WhiteBook (ITSEC) и другие стандарты по информационной безопасности	6	2	2	7	1-4	Самостоятельное изучение рекомендуемых источников и материалов, подготовка к семинарскому занятию.	Т, ПЗ, КР, К
5	2.2. Национальные стандарты по информационной безопасности. **Содержание**: Национальные стандарты РФ (ГОСТы) информационной безопасности. Национальные стандарты РФ ГОСТ-ИСО/МЭК по информационной безопасности. Стандарт Центробанка России «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения».	4	2	2	7,8	1-4	Самостоятельное изучение рекомендуемых источников и материалов, тестирование, выполнение теста, подготовка к семинарскому занятию.	Т, ПЗ, КР, К
	Всего:	18	10	8	35,8			

ПЗ –практическое задание (или семинар), Т – тест, КР – выполнение контрольной самостоятельной работы (темы см. выше), К- коллоквиум,

Приложение 2

Рейтинг – план дисциплины

Международные и российские акты и стандарты по информационной безопасности

Направление подготовки **10.03.01 Информационная безопасность**

Курс 3, семестр 5

Виды учебной деятельности студентов	**Балл за конкретное задание**	**Число заданий за семестр**	**Баллы**	
			Минимальный	**Максимальный**
Модуль 1				
Текущий контроль				**25**
1.Аудиторная работа				
- Практические задания/доклады	3	5	0	15
- устный опрос	2	5	0	10
Рубежный контроль				**25**
Тест 1	0,3	30	0	9
Тест 2	0,3	40	0	12
Тест 3	0,4	10	0	4
Всего				**50**
Модуль 2				
Текущий контроль				**25**
1.Аудиторная работа				
- Практические задания/доклады	3(4)	4	0	13
- Устный опрос	3	4	0	12
Рубежный контроль				**25**
- Итоговый тест	0,25	20	0	10
Контрольная самостоят.работа	5	1	0	5
Собеседование	15	15	0	15
Всего				**50**
Поощрительные баллы				
1.Публикация научной статьи	5	1	0	5
2.Участие в научно-практической конференции по профилю	5	1	0	5
Всего				**10**
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение лабораторных занятий	-	-	0	-10