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

Актуализировано:
на заседании кафедры
протокол № 10 от «7» июня 2018 г.
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.Б.31.02 (базовая)

Программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация
Технологии защиты информации в правоохранительной сфере

Квалификация
Специалист по защите информации

Разработчик (составитель)
Доцент, канд.филос.наук / МироноваН.Г.

Для приема: 2016 г.

Уфа 2018 г.

Составитель: Н.Г.Миронова

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью протокол № 10 от «7» июня 2018 г.

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

Заведующий кафедрой /Исмагилова А.С.

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	1. Знать лексический и грамматический минимум в объеме, необходимом для работы с иноязычными текстами профессиональной направленности и осуществления взаимодействия на иностранном языке.	**ОК-11.** Способность к деловому общению, профессиональной коммуникации на одном из иностранных языков.	
	1. Знать тенденции в области развития информационных систем и динамику проблем информационной безопасности. 2. Знать общеметодологические принципы теории информационной безопасности и состояние законодательной базы и стандарты в области информационной безопасности.	**ПК-18.** Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.	
	1. Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации 2. Знать также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области. 3. Знать методы и средства правовой защиты государственной тайны и информационной безопасности.	**ПК-19.** Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности**.**	
	1. Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области 2. Знать особенности традиционного и безбумажного документооборота 3. Знать принципы решения задач проектирования профессионально-ориентированных программных систем с использованием различных методов и решений.	**ПК-29** - Способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации.	
Умения	1. Уметь читать и переводить иноязычную литературу по профилю направления подготовки, взаимодействовать и общаться на иностранном языке.	**ОК-11.** Способность к деловому общению, профессиональной коммуникации на одном из иностранных языков.	

	1. Уметь использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия, обеспечивающие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС.	**ПК-18.** Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.	
	1. Уметь использовать в практической деятельности правовые знания 2. Уметь анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности. 3. Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности. 4. Уметь предвидеть юридические опасности и угрозы и соблюдать основные правовые требования информационной безопасности, в т.ч. для защиты государственной тайны.	**ПК-19.** Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности**.**	
	1. Уметь подготавливать все виды конфиденциальных документов. 2. Уметь выполнять все виды работ (прием, передачу, хранение, размножение и т.п.) по конфиденциальному делопроизводству. 3. Уметь создавать различные схемы организации защиты документооборота на предприятии. 4. Уметь разрабатывать и включать различные типы автоматизированных систем в традиционный и безбумажный документооборот.	**ПК-29** - Способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации.	
Навыки, опыт деятельности	Владеть одним из иностранных языков на уровне основ профессиональной коммуникации.	**ОК-11.** Способность к деловому общению, профессиональной коммуникации на одном из иностранных языков.	
	1.Владеть навыками выявления и устранения угроз информационной безопасности. 2. Владеть выполнять основные этапы решения задач информационной безопасности; обосновывать организационно-технические мероприятия по защите информации.	**ПК-18.** Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.	
	1. Владеть основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации. 2. Владеть навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности. 3. Владеть навыками поиска нормативной правовой информации необходимой для профессиональной деятельности. 4. Владеть навыками обеспечения и соблюдения режима секретности.	**ПК-19.** Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности**.**	
	1. Владеть методами сбора и анализа исходных данных для проектирования систем защиты	**ПК-29** - Способность формировать рабочую техническую документацию	

	информации 2. Владеть основными методами определения требований, сравнительного анализа подсистем по показателям информационной безопасности	с учетом действующих нормативных и методических документов в области безопасности информации.	

2. Цель и место дисциплины в структуре образовательной программы

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

Дисциплина «Международные и российские акты и стандарты по информационной безопасности» изучается на 4-м курсе в 8 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 ОК-11, ПК-18, ПК-19, ПК-29, сформированные в рамках изучения следующих дисциплин и видов практики: Введение в специальность, Документоведение, Защита информационных процессов в компьютерных системах, Иностранный язык, Информационное право, Правовая защита информации, Правовая охрана результатов интеллектуальной деятельности, Теория информационной безопасности и методология защиты информации, Технологии защищенного документооборота, Электронный документооборот, 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 А.

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

ОК-11. Способность к деловому общению, профессиональной коммуникации на одном из иностранных языков.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап	1. Знать лексический и грамматический минимум в объеме, необходимом для работы с иноязычными текстами	Не знает, не знает иностранной терминологии в области ИБ	Демонстрирует фрагментарные знания при знакомстве с источниками и нормативными документами на иностранном	Испытывает затруднения при работе с нерусскоязычными источниками, ресурсами, документами, с трудом	Демонстрирует целостные, системные знания, терминологию в указанной сфере, свободно ориентируется в

	профессиональной направленности и осуществления взаимодействия на иностранном языке.		(английском) языке или испытывает большие затруднения в понимании иностранной терминологии в сфере ИБ.	ориентируется в иностранной терминологии по информационной безопасности	них при решении практических задач.
Второй этап	1. Уметь читать и переводить иноязычную литературу по профилю направления подготовки, взаимодействовать и общаться на иностранном языке.	Не способен освоить материал или ресурс, если он на иностранном языке	Слабо демонстрирует указанные умения и знания при необходимости ознакомиться с материалами, стандартами, нормативами на иностранном (английском) языке.	Испытывает затруднения при работе с нерусскоязычными источниками, ресурсами, документами, но справляется.	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации
Третий этап	1. Владеть одним из иностранных языков на уровне основ профессиональной коммуникации.	Не владеет навыком при необходимости освоить материал или ресурс на иностранном языке	Слабо демонстрирует указанные навыки при работе с правовыми документами, информационно-справочными системами, программами с нерусско-язычным интерфейсом.	Затрудняется с использованием навыков чтения на английском или ином языке при необходимости изучить и использовать материалы.	Демонстрирует уверенное, свободное владение иностранным языком при решении профессиональных задач.

ПК-18. Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Неудовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап	1. Знать тенденции в области развития информационных систем и динамику проблем информационной безопасности. 2. Знать общеметодологические принципы теории информационной безопасности и состояние законодательной базы и стандарты в области информационной безопасности.	Не демонстрирует указанных знаний	Демонстрирует фрагментарные знания.	Демонстрирует хорошее знание, но с трудом ориентируется в них при решении практических задач или знание - несколько устаревшее, утратившее актуальность.	Демонстрирует целостные, системные знания в указанной сфере, свободно ориентируется в них при решении практических задач.

Второй этап	1. Уметь использовать базовые возможности информационных систем для решения задач фирмы и внедрять компоненты АИС предприятия, обеспечивающие информационную безопасность и достижение стратегических целей и организовать поддержку обеспечения выполнения этой организацией своих функций на основе безопасных АИС.	Не умеет	Слабо демонстрирует указанные умения и знания, без связи навыками решения задач организации службы защиты информации.	Демонстрирует хорошее теоретическое знание компетенции, но недостаточное владение практической стороной при решении задач организации службы защиты информации.	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации
Третий этап	1.Владеть навыками выявления и устранения угроз информационной безопасности. 2. Владеть выполнять основные этапы решения задач информационной безопасности; обосновывать организационно-технические мероприятия по защите информации.	Не владеет и не имеет теоретических знаний об этой сфере	Слабо демонстрирует указанные навыки и знания.	Демонстрирует хорошее владение компетенцией, но имеет устаревшие и малоактуальные сведения.	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации.

ПК-19 - Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности**.**

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Неудовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап	1. Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации 2. Знать также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и	Не демонстрирует указанных знаний	Демонстрирует фрагментарные знания.	Демонстрирует хорошее знание, но с трудом ориентируется в них при решении практических задач или знание - несколько устаревшее, утратившее актуальность.	Демонстрирует целостные, системные знания в указанной сфере, свободно ориентируется в них при решении практических задач.

	экспортному контролю в данной области. 3. Знать методы и средства правовой защиты государственной тайны и информационной безопасности.				
Второй этап	1. Уметь использовать в практической деятельности правовые знания 2. Уметь анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности. 3. Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности. 4. Уметь предвидеть юридические опасности и угрозы и соблюдать основные правовые требования информационной безопасности, в т.ч. для защиты государственной тайны.	Не умеет	Слабо демонстрирует указанные умения и знания, без связи навыками решения задач организации службы защиты информации.	Демонстрирует хорошее теоретическое знание компетенции, но недостаточное владение практической стороной при решении задач организации службы защиты информации.	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации
Третий этап	1. Владеть основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации. 2. Владеть навыками работы с нормативными правовыми актами, нормативной и технической информацией,	Не владеет и не имеет теоретических знаний об этой сфере	Слабо демонстрирует указанные навыки и знания.	Демонстрирует хорошее владение компетенцией, но имеет устаревшие и малоактуальные сведения.	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации.

	необходимой для профессиональной деятельности. 3. Владеть навыками поиска нормативной правовой информации необходимой для профессиональной деятельности. 4. Владеть навыками обеспечения и соблюдения режима секретности.				

ПК-29 - Способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Неудовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап	1. Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области 2. Знать особенности традиционного и безбумажного документооборота 3. Знать принципы решения задач проектирования профессионально-ориентированных программных систем с использованием различных методов и решений.	Не демонстрирует указанных знаний	Демонстрирует фрагментарные знания.	Демонстрирует хорошее знание, но с трудом ориентируется в них при решении практических задач или знание - несколько устаревшее, утратившее актуальность.	Демонстрирует целостные, системные знания в указанной сфере, свободно ориентируется в них при решении практических задач.
Второй этап	1. Уметь подготавливать все виды конфиденциальных документов. 2. Уметь выполнять все виды работ (прием,	Не умеет	Слабо демонстрирует указанные умения и знания, без связи навыками	Демонстрирует хорошее теоретическое знание компетенции, но недостаточное владение	Демонстрирует уверенное, свободное владение указанными навыками при решении задач

	передачу, хранение, размножение и т.п.) по конфиденциальному делопроизводству. 3. Уметь создавать различные схемы организации защиты документооборота на предприятии. 4. Уметь разрабатывать и включать различные типы автоматизированных систем в традиционный и безбумажный документооборот.		решения задач организации службы защиты информации.	практической стороной при решении задач организации службы защиты информации.	организации службы защиты информации
Третий этап	1. Владеть методами сбора и анализа исходных данных для проектирования систем защиты информации 2. Владеть основными методами определения требований, сравнительного анализа подсистем по показателям информационной безопасности	Не владеет и не имеет теоретических знаний об этой сфере	Слабо демонстрирует указанные навыки и знания.	Демонстрирует хорошее владение компетенцией, но имеет устаревшие и малоактуальные сведения.	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации.

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 лексический и грамматический минимум в объеме, необходимом для работы с иноязычными текстами профессиональной направленности и осуществления взаимодействия на иностранном языке.	**ОК-11.** Способность к деловому общению, профессиональной коммуникации на одном из иностранных языков.	опрос
	Знание правовых норм, стандартов лицензирования, правовых основ организации в области обеспечения защиты гос.тайны и сертификации средств защиты информации и конфиденциальной информации, знание системы организации бумажного и электронного конфиденциального делопроизводства, документооборота.	**ПК-29** - Способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации.	Опрос, практические задания, коллоквиум, тесты
	Знать тенденции в области развития информационных систем и динамику проблем информационной безопасности	**ПК-18.** Способность разрабатывать предложения по совершенствованию системы управления безопасностью	Опрос, практические задания, коллоквиум,

		информации.	тесты
	Знание основных нормативных и правовых актов в области информационной безопасности и защиты информации, нормативных методических документов Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области. Знание методов и средств правовой защиты государственной тайны и информационной безопасности.	**ПК-19.** Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности**.**	Опрос, практические задания, коллоквиум, тесты
2-й этап Умения	Уметь читать и переводить иноязычную литературу по профилю направления подготовки, взаимодействовать и общаться на иностранном языке.	**ОК-11**. Способность к деловому общению, профессиональной коммуникации на одном из иностранных языков.	Опрос, практические задания, коллоквиум, тесты
	Навык использования базовых возможностей информационных систем для решения задач фирмы и организации выполнения организацией своих функций на основе безопасных АИС.	**ПК-18.** Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.	Опрос, практические задания, коллоквиум, тесты
	Умение использовать в практической деятельности правовые знания, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности. Умение анализировать и составлять основные правовые акты, делать правовую оценку информации в профессиональной деятельности, предвидеть юридические опасности и угрозы, соблюдать основные правовые требования информационной безопасности.	**ПК-19.** Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности**.**	Опрос, практические задания, коллоквиум, тесты
	Умение находить нужную информацию, выбирать необходимые информационные ресурсы и источники знаний в электронной среде, определять зависимость между затратами на ИБ и уровнем защищенности; подготавливать и использовать конфиденциальные документы, в т.ч. в безбумажном документообороте.	**ПК-29** - Способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации.	Опрос, практические задания, коллоквиум, тесты
3 этап - владения, навыки	Владеть навыками выявления и устранения угроз информационной безопасности	**ПК-18.** Способность разрабатывать предложения по совершенствованию системы управления безопасностью информации.	Опрос, практические задания, коллоквиум, тесты
	Владение навыками работы с нормативными правовыми актами, навыками самостоятельного анализа	**ПК-19.** Способность соблюдать в профессиональной деятельности требования	Опрос, практические задания,

	правовой информации, анализа юридических последствий, связанных с использованием информации, навыками лицензирования в области защиты информации, методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности. Владение навыками поиска нормативной правовой информации необходимой для профессиональной деятельности, обеспечения и соблюдения режима секретности.	нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности**.**	коллоквиум, тесты
	Владение навыками обоснования проектных решений по созданию систем обеспечения безопасности информации, методами сбора и анализа исходных данных для проектирования систем защиты информации, владение методами определения требований, сравнительного анализа подсистем по показателям информационной безопасности	**ПК-29** - Способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации.	Опрос, практические задания, коллоквиум, тесты

Формы и виды контроля:

Типовые материалы к экзамену

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.

Структура экзаменационного билета.

Экзаменационный билет состоит из двух теоретических и одного практического вопросов.
Образец экзаменационного билета:

Федеральное государственное бюджетное образовательное учреждение высшего образования
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт истории и государственного управления

Специальность 10.05.05 «Безопасность информационных технологий в правоохранительной деятельности»
Дисциплина «Международные и российские акты и стандарты по информационной безопасности»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Конституция РФ, федеральные законы и кодексы в области защиты информации.

2. Маркировка сертифицированной продукции.
3. Практический вопрос: ИСПДн государственного учреждения обрабатывает определенные категории ПД граждан и требует обеспечения 1 уровня защищенности. Какие нормативные документы следует учитывать при построении системы защиты информации этого ИСПДн? Какие выводы об описании ИСПДн можно сделать из предоставленной информации?

Зав. кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии оценивания результатов экзамена: При выставлении баллов именно за экзамен (до 30 баллов в дополнение к баллам, полученным за другие виды отчетности) действует такой критерий оценки:

25-30 баллов

Студент дал полные, развернутые ответы на теоретический вопрос билета и правильно выполнил практическое задание, продемонстрировал знание функциональных возможностей, терминологии, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок.

17-24 баллов

Студент раскрыл в основном теоретический вопрос, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки, но все задание выполнено до конца.

10-16 баллов

При ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент сделал практическое задание лишь частично.

1-10 баллов

Ответ на теоретический вопрос свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Студент не смог ответить ни на один дополнительный вопрос

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей дисциплины, перечисленных в рейтинг-плане дисциплины, для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10.

Шкалы оценивания для экзамена: перевод оценки из 100-балльной в 4-балльную производится следующим образом:

- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов);
- хорошо – от 60 до 79 баллов;
- удовлетворительно – от 45 до 59 баллов;
- неудовлетворительно – менее 45 баллов.

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 6 баллов (1 правильно сделанный вопрос теста = 0,2 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 5 баллов (1 правильно сделанный вопрос теста = 0,125 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 4 баллов (1 правильно сделанный вопрос теста = 0,2 балла).

Подробнее тесты приведены в ФОС.

Типовые темы практических занятий

Практическое занятие 1. Законодательство РФ в области информационной безопасности.

Цель занятия: знакомство с перечнем регуляторов, занимающихся обеспечением контроля в сфере информационной безопасности, а также с основными федеральными законами РФ в сфере информационной безопасности.

Содержание занятия: ознакомление с перечнем, текстом и основными положениями законов.

Список тем для изучения:

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.

Методические указания:

Руководствуясь перечнем заданий, ИС Консультант плюс, доступом к сайтам ФСТЭК и ФСБ, материалами лекционных занятий, проделать следующее:

- ознакомиться с нормативно-правовой базой,
- уяснить термины и основные положения в соответствии с темой и содержанием занятия,
- при необходимости сделать краткий обзор в виде доклада или конспекта (критерии оценки этой работы см. ниже),
- изложить конспект устно,
- ответить на вопросы по тексту нормативных актов и документов (перечень вопросов приводится ниже, подробнее – в ФОС, критерии оценки ответа на устный вопрос приводятся там же),
- выполнить задание на поиск определенных положений в тексте нормативных актов.
- Отчет при необходимости оформить письменно в электронной форме.

Практические занятия 2-3. Правовые основы защиты информации, коммерческой и государственной тайны. Тест 1.

Цель занятия: знакомство с основными федеральными законами РФ в сфере информационной безопасности в сфере коммерческой и государственной тайны.

Содержание занятия: ознакомление с перечнем, текстом и основными положениями законов. Во второй части занятий – тестирование – 1 акад.час.

1. Понятие конфиденциальной информации.
2. Виды тайны.

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

Методические указания:
Руководствуясь перечнем заданий, ИС Консультант плюс, доступом к сайтам ФСТЭК и ФСБ, материалами лекционных занятий, проделать следующее:
- ознакомиться с нормативно-правовой базой,
- уяснить термины и основные положения в соответствии с темой и содержанием занятия,
- при необходимости сделать краткий обзор/конспект,
- изложить конспект устно,
- ответить на вопросы по тексту нормативных актов и документов,
- выполнить задание на поиск определенных положений в тексте нормативных актов.
- пройти тестирование по **тесту 1**.

Практические занятия 4-5. Изучение положений о государственном лицензировании деятельности в области защиты информации. Тест 2.

Цель занятия: знакомство с перечнем регуляторов, занимающихся обеспечением контроля в сфере информационной безопасности, из функциями, а также с основными приказами, методическими документами и положениями регуляторов и органов власти в сфере информационной безопасности.

Содержание занятия: ознакомление с перечнем, текстом и основными положениями законов, методических документов, приказов, распоряжений. Тестирование.

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.
8. **Тест 2**.

Методические указания:
Руководствуясь перечнем заданий, ИС Консультант плюс, доступом к сайтам ФСТЭК и ФСБ, материалами лекционных занятий, проделать следующее:
- ознакомиться с нормативно-правовой базой,
- уяснить термины и основные положения в соответствии с темой и содержанием занятия,
- при необходимости сделать краткий обзор/конспект,
- изложить конспект устно,
- ответить на вопросы по тексту нормативных актов и документов,
- выполнить задание на поиск определенных положений в тексте нормативных актов.
- пройти тестирование по **тесту 2**.

Практическое занятие 6. 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.

Методические указания:
Руководствуясь перечнем заданий, ИС Консультант плюс, доступом к сайтам ФСТЭК и ФСБ, материалами лекционных занятий, проделать следующее:
- ознакомиться с нормативно-правовой базой,
- уяснить термины и основные положения в соответствии с темой и содержанием занятия,
- при необходимости сделать краткий обзор в виде доклада или конспекта (критерии оценки этой работы см. ниже),
- изложить конспект устно,
- ответить на вопросы по тексту нормативных актов и документов (перечень вопросов приводится ниже, подробнее – в ФОС, критерии оценки ответа на устный вопрос приводятся там же),
- выполнить задание на поиск определенных положений в тексте нормативных актов.
- Отчет при необходимости оформить письменно в электронной форме.

Практическое занятие 7. 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.

Методические указания:
Руководствуясь перечнем заданий, ИС Консультант плюс, доступом к сайтам ФСТЭК и ФСБ, материалами лекционных занятий, проделать следующее:
- ознакомиться с нормативно-правовой базой,
- уяснить термины и основные положения в соответствии с темой и содержанием занятия,
- при необходимости сделать краткий обзор/конспект,
- изложить конспект устно,
- ответить на вопросы по тексту нормативных актов и документов,
- выполнить задание на поиск определенных положений в тексте нормативных актов.
- Отчет при необходимости оформить письменно в электронной форме.

Практические занятия 8-9. Система сертификации средств криптографической защиты информации.

Цель занятия: знакомство с функциями ФСБ и их лицензиатов в сфере криптозащиты информации, с перечнем и содержанием положений и методических материалов ФСБ в области криптографии.

Содержание занятия: ознакомление с перечнем, текстом и основными положениями законов, нормативных актов и методических документов ФСТЭК и ФСБ по криптозащите информации. Тестирование

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

Методические указания:
Руководствуясь перечнем заданий, ИС Консультант плюс, доступом к сайтам ФСТЭК и ФСБ, материалами лекционных занятий, проделать следующее:
- ознакомиться с нормативно-правовой базой,
- уяснить термины и основные положения в соответствии с темой и содержанием занятия,
- при необходимости сделать краткий обзор/конспект,
- изложить конспект устно,
- ответить на вопросы по тексту нормативных актов и документов,
- выполнить задание на поиск определенных положений в тексте нормативных актов.
- пройти тестирование по **тесту 3**.

Модуль 2. Международные и национальные стандарты по информационной безопасности

Практическое занятие 10. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации.

Цель занятия: знакомство с перечнем международных и отечественных стандартов, соглашений в сфере информационной безопасности, а также нормативные документы, касающиеся порядка аттестации объектов информатизации по требованиям ИБ.

Содержание занятия: ознакомление с перечнем, текстом и основными положениями нормативных документов.

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.

Методические указания:
Руководствуясь перечнем заданий, ИС Консультант плюс, доступом к сайтам ФСТЭК и ФСБ, материалами лекционных занятий, проделать следующее:
- ознакомиться с нормативно-правовой базой,
- уяснить термины и основные положения в соответствии с темой и содержанием занятия,
- при необходимости сделать краткий обзор в виде доклада или конспекта (критерии оценки этой работы см. ниже),
- изложить конспект устно,

- ответить на вопросы по тексту нормативных актов и документов (перечень вопросов приводится ниже, подробнее – в ФОС, критерии оценки ответа на устный вопрос приводятся там же),
- выполнить задание на поиск определенных положений в тексте нормативных актов.
- Отчет при необходимости оформить письменно в электронной форме.

Практические занятия 11-12. Коллоквиум по индивидуальным темам.

Вопросы коллоквиума:

1. Стандарт Центробанка России от 01.06.2014 г. «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения» (СТО БР ИББС-1.0–2014)
2. Использование грифов секретности.
3. Окинавская «Хартия глобального информационного общества»;
4. Директива по безопасности информационных систем и сетей ОЭСР 2002 г.«К культуре безопасности» ОЭСР и принципы операционного риска Банка международных расчетов(Basel II).
5. Стандарты ISO/IEC 17799:2005, ISO/IEC 27000, ISO/IEC 27001:2005, ISO/IEC 27002,ISO/IEC 27005;
6. Стандарты DOD , TCSEC (оранжевая книга) США, GreenBook Германия,WhiteBook (ITSEC)
7. РД «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»
8. Классы защищенности АС от НСД к информации. Требования по защите информации от НСД для АС.
9. Классы защищенности СВТ и МЭ. Показатели защищенности СВТ.
10. СТР-К
11. Национальные стандарты РФ ГОСТ-ИСО/МЭК по информационной безопасности;
12. ГОСТ Р ИСО/МЭК 15408-2002. Профиль защиты и задание по безопасности.
13. ГОСТ Р ИСО/МЭК 15408-2002. Функциональные требования безопасности.
14. ГОСТ Р ИСО/МЭК 15408-2002. Оценочные уровни доверия.
15. ГОСТ Р ИСО/МЭК 15408-2002. Область применения документа, краткий обзор.

Критерии оценки работы на коллоквиуме.

Студент может подготовить до 2 вопросов коллоквиума, ответ на каждый из вопросов оценивается по следующему принципу:
- 0 баллов – если студент не подготовил и не дал на вопрос правильного ответа
- 1 балл – если излагаемый студентом материал утратил свою актуальность.
- 2 балла – если ответ студента на вопрос неполон или излагаемый материал частично утратил свою актуальность.
- 3 балла – если ответ на вопрос коллоквиума полный и правильный.

Практические занятия 14-15. Изучение особенностей аттестации помещений по требованиям безопасности информации. Тестирование 4.

Цель занятия: знакомство с порядков аттестации защищенных помещений по требованиям безопасности информации различного уровня защищенности.

Содержание занятия: ознакомление с перечнем, текстом и основными положениями нормативных документов. Итоговое тестирование.

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

5. Отчет по результату выполнения контрольной самостоятельной работы (защита КСР)
6. Итоговое тестирование (Тест 4).

Методические указания:
Руководствуясь перечнем заданий, ИС Консультант плюс, доступом к сайтам ФСТЭК и ФСБ, материалами лекционных занятий, проделать следующее:
- ознакомиться с нормативно-правовой базой,
- уяснить термины и основные положения в соответствии с темой и содержанием занятия,
- при необходимости сделать краткий обзор/конспект,
- изложить конспект устно,
- ответить на вопросы по тексту нормативных актов и документов,
- выполнить задание на поиск определенных положений в тексте нормативных актов.
- пройти тестирование по **тесту 4**.

Практическое занятия 16. Защита контрольных самостоятельных работ

Темы, метод.указания и критерии оценки КСР см. ниже.

Критерии и методика оценивания результатов 1-15 практического занятий (в баллах), без учета оценки результатов устного опроса**:**

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 ОК-11:

ОК-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-18:

ПК-18 – 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-18 – 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-18 – I.У

Определение требований к защите и категорирование ресурсов.

ПК-18 – I.У

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

ПК-18 – 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-18 – II.У

Классы защищенности согласно «Оранжевой книге»

ПК-18 – I.В

Сравнение основных справочно-правовых систем.

ПК-18 – II.В

Написание доклада на тему «Современные средства антивирусной защиты»

Примерные вопросы для проверки знаний по компетенции ПК-19:

ПК-19 – I.З
- Порядок проведения аттестации ИС и ИСПДн.
- Каким нормативным актом/постановлением описывается порядок определения уровней защищённости персональных данных?

ПК-19 – 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-19 – II.У

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

ПК-19 – I.В

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

ПК-19 – II.В

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

ПК-19 – 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-19 – II.В

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

Примерные вопросы для проверки знаний по компетенции ПК-29:

ПК-29 – I.З

- Законодательная база защиты документированной информации в РФ – назовите известные вам ГОСТы, законы, постановления, директивы и т.п. с краткой характеристикой.
- Что понимается под «специальными проверками» технических средств?
- Перечислите актуальные на сегодня подзаконные нормативно-правовые акты в сфере защиты информации (с краткой их характеристикой).

ПК-29 – I.У

С использованием СПС «Гарант» найти постановление Правительства РФ от 23 апреля 2004 г. № 219.

ПК-29 – I.У

Определение требований к защите и категорирование ресурсов.

ПК-29 – I. В

Используя актуальные документы ФСТЭК, ФСБ, составьте перечень угроз информационной безопасности для малого производственного предприятия;

ПК-29 – II. В

Используя актуальные документы ФСТЭК, ФСБ, составьте перечень уязвимостей объектам информатизации для государственного учреждения.

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).

Методические указания по выполнению Контрольной самостоятельной работы

Цель КСР: получение практических навыков использования нормативно-правовых и методических документов при осуществлении профессиональной деятельности по созданию и обеспечению системы защиты информации в организациях.

Методические указания: 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.

4.3. Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении Б.

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. Аверченков В.И., Рытов М.Ю., Кувыклин А.В., Гайнулин Т.Р. Разработка системы технической защиты информации: учебное пособие. - М.: Флинта, 2011. – 187 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=93349&sr=1
6. Анализ состояния защиты данных в информационных системах: учебно-методическое пособие. - Новосибирск: НГТУ, 2012. – 52 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=228844&sr=1
7. Анисимов А.А. Менеджмент в сфере информационной безопасности: Учебное пособие. - М.: Интернет-Университет Информационных Технологий, 2009. – 176 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=232981&sr=1
8. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации: Учебное пособие. – М.: Академия. – 2011 с. - Режим доступа: https://bashedu.bibliotech.ru/Reader/Book/2013080217381731971500009579
9. Слепова И.Б. Информация как объектотношений собственности. -М.: Лаборатория книги, 2011. – 102 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=140255&sr=1

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

1. Электронная библиотечная система БашГУ – www.bashlib.ru
2. Электронная библиотечная система «ЭБ БашГУ» - https://elib.bashedu.ru

3. Электронная библиотечная система «Университетская библиотека онлайн» - https://biblioclub.ru
4. Электронная библиотечная система издательства «Лань» - https://e.lanbook.com
5. Словари и энциклопедии On-Line- http://www.dic.academic.ru
6. Справочная правовая система «КонсультантПлюс» - http://www.consultant-plus.ru
7. Антиплагиат.ВУЗ. Договор № 81 от 27.04.2018 г. Срок действия лицензии до 04.05.2019 г., договор № 1104 от 18.04.2019 г. Срок действия лицензии до 04.05.2020 г
8. Справочная правовая система Консультант Плюс. Договор №31705775411 от 07.12.2017 г.
9. База данных «Вестники Московского университета» (на платформе East View) (вход без регистрации). - Ссылка http://www.ebiblioteka.ru/browse/udb/12.
10. База данных «Издания по общественным и гуманитарным наукам» (на платформе East View) - Ссылка http://www.ebiblioteka.ru (вход из сети вуза без регистрации).
11. Электронная база данных диссертаций РГБ (авторизованный доступ по паролю в сети вуза) – Ссылка: http://dvs.rsl.ru
12. Web of Science - наукометрическая, библиографическая и реферативная база данных издательской корпорации Thomson Reuters. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://apps.webofknowledge.com/
13. SCOPUS - наукометрическая, библиографическая и реферативная база данных издательской корпорации Elsevier. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://www.scopus.com/
14. Computers & Applied Sciences Complete (EBSCO) - доступ в сети вуза, язык английский. - Ссылка: http://search.ebscohost.com/
15. Annual Reviews – обзор журналов по общественно-научной тематике и др. – доступ из сети вуза. – Ссылка: http://www.annualreviews.org/
16. Taylor and Francis – База полнотекстовых научных журналов, книг. Язык английский. – доступ из сети вуза. – Ссылка: http://www.tandf
17. Wiley - Полнотекстовая база данных статей из 1400 журналов издательства Wiley по всем отраслям знаний. Язык английский. Доступ из сети вуза без регистрации. – Ссылка: http://onlinelibrary.wiley.com/
18. Нормативные документы и материалы сайта ФСТЭК России (Федеральной службы по техническому и экспортному контролю России): https://fstec.ru/ Раздел Национальные старты информационной безопасности: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty
19. Банк данных "Копии правовых актов: Российская Федерация» - http://giod.consultant.ru/
20. Национальные стандарты РФ в области информационной безопасности: http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii

Программное обеспечение:

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.
4. Правовая система «КонсультантПлюс». Договор №28826 от 09.01.2019 г. Лицензии бессрочные.

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
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 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). **3.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус),	Лекции, практические 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 MA1225 – 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 MA1225 – 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 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 IN-TEL 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 № 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). **4.** ***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). **5.** ***помещения для самостоятельной работы:*** аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).		**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 **Программное обеспечение:** 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. 4. Правовая система «КонсультантПлюс». Договор №28826 от 09.01.2019 г. Лицензии бессрочные.

Приложение А

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 8 семестр ОФО

Рабочую программу осуществляют:
Лекции: ст. преподаватель А.М. Оводов
Практические занятия: ст. преподаватель А.М. Оводов

Вид работы	Объем дисциплины
	ОФО
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	49,2
лекций	16
практических/ семинарских	32
лабораторных	
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	42
Учебных часов на подготовку к экзамену (Контроль)	52,8
Форма контроля	Экзамен 8 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	3	4	5	6	7	8	9
	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	6		8	1-9	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	4	6		8	1-9	Самостоятельное изучение рекомендуемых источников и материалов, подготовка к семинарскому занятию.	Т, ПЗ, КР, К

	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, 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	6		8	1-9		Т, ПЗ, КР, К
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	4	6		8	1-9		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	8		10	1-9	Самостоятельное изучение рекомендуемых источников и материалов, тестирование, выполнение теста, подготовка к семинарскому занятию.	Т, ПЗ, КР, К
	Всего:	16	32	-	42			

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

Приложение Б

Рейтинг – план дисциплины

Международные и российские акты и стандарты по информационной безопасности

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Курс 4, семестр 8 2018/2019 гг.

Виды учебной деятельности студентов	**Балл за конкретное задание**	**Число заданий за семестр**	**Баллы**	
			Минимальный	**Максимальный**
Модуль 1				
Текущий контроль				**20**
1.Аудиторная работа				
- Практические задания/доклады	2	5	0	10
- устный опрос	2	5	0	10
Рубежный контроль				**15**
Тест 1	0,2	30	0	6
Тест 2	0,125	40	0	5
Тест 3	0,4	10	0	4
Всего				**35**
Модуль 2				
Текущий контроль				**20**
1.Аудиторная работа				
- Практические задания/доклады	2	5	0	10
- Устный опрос	2	5	0	10
Рубежный контроль				**15**
- коллоквиум	3	2	0	6
- Итоговый тест	0,2	20	0	4
Контрольная самостоят.работа	5	1	0	5
Всего				**35**
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
Итоговый контроль				
Экзамен	30	1	0	**30**