



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)

Защита персональных данных

Б1.В.1.ДВ.10.02 (Вариативная)

программа бакалавриата

Направление
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации

Квалификация
бакалавр

Разработчик (составитель)
к.х.н.

 / А.А. Султанова

Для приема: 2015 г.

Уфа 2018 г.

Составитель: А.А. Султанова

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

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры государственного управления, протокол № __ от «__» _____ 201_ 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 (модулю), соотнесенных с планируемыми результатами освоения образовательной программы	4
2. Цель и место дисциплины (модуля) в структуре образовательной программы	6
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)	6
4. Фонд оценочных средств по дисциплине	7
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	7
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	10
4.3. Рейтинг-план дисциплины	12
5. Учебно-методическое и информационное обеспечение дисциплины	18
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	18
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины	18
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	19

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ	– способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)	
	принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации	– способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)	
	политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	– способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)	
	определять цели и задачи проведения экспериментальных исследований	– способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)	
	нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	– способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)	
	общеметодологические принципы теории информационной безопасности	– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПСК-2)	
Умения	ориентироваться в нормативно-правовых	– способностью использовать нормативные правовые акты в	

	актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	профессиональной деятельности (ОПК-5)	
	осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	– способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)	
	реализовывать на практике принципы политики безопасности	– способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)	
	ориентироваться в современной технике и технологиях с целью их освоения и внедрения для решения поставленной задачи	– способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)	
	анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности	– способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)	
	обосновывать организационно-технические мероприятия по защите информации	– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПСК-2)	
Владения (навыки / опыт деятельности)	навыками анализа юридических последствий, связанных с использованием информации	– способностью использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)	
	методами и средствами выявления угроз безопасности автоматизированным	– способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)	

	системам		
	навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	– способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)	
	навыками анализа и интерпретации полученных результатов	– способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12)	
	навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности	– способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)	
	навыками обоснования, выбора, реализации и контроля результатов управленческого решения	– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПСК-2)	

2. Цель и место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Защита персональных данных» относится к вариативной части образовательной программы.

Дисциплина изучается на 4 курсе в 7-м семестре.

Цели изучения дисциплины: изучение различных видов угроз информационным ресурсам, представляющим собой персональные данные, каналов утечки информации, модели нарушителя и его потенциальных возможностей по несанкционированному доступу и съему информации, изучение принципов моделирования угроз безопасности персональных данных, практическое освоение принципов построения системы технической защиты информации ограниченного доступа.

Изучение дисциплины базируется на знаниях, умениях и навыках, сформированных в результате освоения студентами предшествующих дисциплин образовательной программы по направлению 10.03.01 Информационная безопасность профиля подготовки «Организация и технология защиты информации»: «Защита информации в системах связи», «Международные и российские нормативные акты и стандарты по информационной безопасности», «Защита и обработка конфиденциальных документов», «Техническая защита информации», «Программно-аппаратные средства защиты информации».

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: способностью использовать нормативные правовые акты в профессиональной деятельности

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 (уровень) Пороговый	Знать: основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ	Не знает	В целом знает основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ, но испытывает трудности при их описании	Знает основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ, но допускает незначительные ошибки при их описании	Знает основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ
Второй этап (уровень) Базовый	Уметь: ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	Не умеет	В целом умеет ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности, но допускает значительные ошибки	Умеет ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности, но допускает незначительные ошибки	Умеет ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности
Третий этап (уровень) Повышенный	Владеть: навыками анализа юридических последствий, связанных с использованием информации	Не владеет	В целом владеет навыками анализа юридических последствий, связанных с использованием информации, но испытывает трудности в условиях конкретной задачи	В целом владеет навыками анализа юридических последствий, связанных с использованием информации, но допускает незначительные ошибки	Владеет навыками анализа юридических последствий, связанных с использованием информации

ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты

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 (уровень) Пороговый	Знать: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации	Не знает	В целом знает принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации, но испытывает трудности при их описании	Знает принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации, но допускает незначительные ошибки при их описании	Знает принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
Второй этап (уровень) Базовый	Уметь: осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Не умеет	В целом осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты, но допускает значительные ошибки	Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты, но допускает незначительные ошибки	Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты

Третий этап (уровень) Повышенный	Владеть: методами и средствами выявления угроз безопасности автоматизированным системам	Не владеет	В целом владеет методами и средствами выявления угроз безопасности автоматизированным системам, но испытывает трудности при описании и допускает ошибки при использовании в условиях конкретной задачи	Владеет методами и средствами выявления угроз безопасности автоматизированным системам, но допускает незначительные ошибки	Владеет методами и средствами выявления угроз безопасности автоматизированным системам
----------------------------------	---	------------	--	--	--

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

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 (уровень) Пороговый	Знать: политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	Не знает	В целом знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, но испытывает трудности при их описании	Знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, но допускает незначительные ошибки при их описании	Знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации
Второй этап (уровень) Базовый	Уметь: реализовывать на практике принципы политики безопасности	Не умеет	В целом умеет реализовывать на практике принципы политики безопасности, но допускает значительные ошибки	Умеет реализовывать на практике принципы политики безопасности, но допускает незначительные ошибки	Реализовывает на практике принципы политики безопасности
Третий этап (уровень) Повышенный	Владеть: навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	Не владеет	В целом владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления, но допускает существенные ошибки	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления, но допускает незначительные ошибки	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления

ПК-12: способностью принимать участие в проведении экспериментальных исследований системы защиты 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 (уровень) Пороговый	Знать: определять цели и задачи проведения экспериментальных исследований	Не знает	В целом знает цели и задачи проведения экспериментальных исследований, но испытывает трудности при их описании	Знает, как определять цели и задачи проведения экспериментальных, но допускает незначительные ошибки при их описании	Знает, как определять цели и задачи проведения экспериментальных
Второй этап (уровень) Базовый	Уметь: ориентироваться в современной технике и технологиях с целью их освоения и внедрения для решения поставленной задачи	Не умеет	В целом умеет ориентироваться в современной технике и технологиях с целью их освоения и внедрения для решения поставленной задачи, но допускает значительные ошибки	Умеет ориентироваться в современной технике и технологиях с целью их освоения и внедрения для решения поставленной задачи, но допускает незначительные ошибки	Умеет ориентироваться в современной технике и технологиях с целью их освоения и внедрения для решения поставленной задачи
Третий этап (уровень)	Владеть: навыками анализа и интерпретации	Не владеет	В целом владеет навыками анализа и интерпретации	Владеет навыками анализа и	Владеет навыками анализа и

Повышенный	полученных результатов		полученных результатов, но испытывает трудности в условиях конкретной задачи	интерпретации полученных результатов, но допускает незначительные ошибки	интерпретации полученных результатов
------------	------------------------	--	--	--	--------------------------------------

ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

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 (уровень) Пороговый	Знать: нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	Не знает	В целом знает нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области, но испытывает трудности при их описании	Знает нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области, но допускает незначительные ошибки при их описании	Знает нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области
Второй этап (уровень) Базовый	Уметь: анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности	Не умеет	В целом умеет анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, но допускает значительные ошибки	Умеет анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, но допускает незначительные ошибки	Умеет анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности
Третий этап (уровень) Повышенный	Владеть: навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности	Не владеет	В целом владеет навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, но испытывает трудности в условиях конкретной организации (органа власти)	Владеет навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, но допускает незначительные ошибки	Владеет навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности

ПСК-2: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью

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 (уровень) Пороговый	Знать: общеметодологические принципы теории информационной безопасности	Не знает	В целом знает общеметодологические принципы теории информационной безопасности, но испытывает трудности при их описании	Знает общеметодологические принципы теории информационной безопасности, но допускает незначительные ошибки при их описании	Демонстрирует целостные знания об общеметодологических принципах теории информационной безопасности

Второй этап (уровень) Базовый	Уметь: обосновывать организационно-технические мероприятия по защите информации	Не умеет	Умеет обосновывать организационно-технические мероприятия по защите информации, но допускает значительные ошибки	Умеет обосновывать организационно-технические мероприятия по защите информации, но допускает незначительные ошибки	Умеет обосновывать организационно-технические мероприятия по защите информации
Третий этап (уровень) Повышенный	Владеть: навыками обоснования, выбора, реализации и контроля результатов управленческого решения	Не владеет	Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения, но допускает ошибки	Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения, но допускает незначительные ошибки	Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины

(для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

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 Знать	основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ	ОПК-5	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
	принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации	ПК-3	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
	политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и	ПК-4	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос

	оптимизации		
	определять цели и задачи проведения экспериментальных исследований	ПК-12	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
	нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области	ПК-15	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
	общеметодологические принципы теории информационной безопасности;	ПСК-2	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
2-й этап	ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности;	ОПК-5	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
Уметь	осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	ПК-3	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
	реализовывать на практике принципы политики безопасность	ПК-4	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
	ориентироваться в современной технике и технологиях с целью их освоения и внедрения для решения поставленной задачи	ПК-12	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
	анализировать и составлять основные правовые акты и осуществлять правовую	ПК-15	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа,

	оценку информации, используемых в профессиональной деятельности		устный индивидуальный опрос
	обосновывать организационно-технические мероприятия по защите информации	ПСК-2	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
3-й этап Владеть	навыками анализа юридических последствий, связанных с использованием информации	ОПК-5	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
	методами и средствами выявления угроз безопасности автоматизированным системам	ПК-3	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
	навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	ПК-4	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
	навыками анализа и интерпретации полученных результатов	ПК-12	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
	навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности	ПК-15	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос
	навыками обоснования, выбора, реализации и контроля результатов управленческого решения	ПСК-2	Устный опрос, дискуссия, тест, контрольная работа, самостоятельная работа, устный индивидуальный опрос

4.3. Рейтинг-план дисциплины

Рейтинг-план дисциплины представлен в приложении 1.

Экзамен

Структура экзаменационного билета

Экзаменационный билет состоит из двух вопросов, отражающих соответственно материал первого и второго модуля.

Типовые экзаменационные материалы

1. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных
2. Нормативное правовое регулирование организации обработки и обеспечения безопасности персональных данных в Российской Федерации
3. Содержание и основные положения Федерального закона «О персональных данных»
4. Меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами
5. Организация работ и назначение ответственных лиц
6. Прием и обработка обращений и запросов субъектов персональных данных или их представителей
7. Права субъекта ПДн
8. Обследование информационных систем организации и описание процессов обработки персональных данных
9. Перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных
10. Проблемные вопросы отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки
11. Определение правового основания обработки персональных данных и прочих сведений, необходимых для регистрации организации в реестре Роскомнадзора
12. Определение Перечня информационных систем персональных данных
13. Определение перечня должностей сотрудников, допущенных к обработке персональных данных в организации
14. Разработка и утверждение документов, определяющих политику оператора в отношении обработки персональных данных и локальных актов по вопросам обработки ПДн
15. Политика в отношении обработки персональных данных в организации
16. Ознакомление работников с порядком обработки и обеспечения безопасности персональных данных
17. Согласие на обработку персональных данных
18. Разъяснение субъекту ПДн юридических последствий отказа предоставить свои ПДн
19. Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных
20. Организация обработки персональных данных, осуществляемой без использования средств автоматизации
21. Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных
22. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных
23. Разработка уведомления об обработке (о намерении осуществлять обработку) персональных данных
24. Осуществление внутреннего контроля соответствия обработки персональных данных установленным требованиям

25. Принятие правовых, организационных и технических мер по обеспечению безопасности ПДн при их обработке
26. Формирование требований к системе защиты персональных данных
27. Угрозы утечки информации по техническим каналам, актуальность, классификация ТКУИ
28. Угрозы несанкционированного доступа к персональным данным, обрабатываемым в информационных системах
29. Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн
30. Определение уровня защищённости персональных данных
31. Состав и содержание мер по обеспечению безопасности персональных данных
32. Разработка системы защиты персональных данных
33. Внедрение системы защиты персональных данных
34. Состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации
35. Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных
36. Обеспечение защиты информации в ходе эксплуатации аттестованной ИСПДн
37. Обеспечение ЗИ при выводе из эксплуатации аттестованной ИСПДн
38. Контроль за соблюдением законодательства Российской Федерации в области персональных данных
39. Ответственность за нарушение законодательства о персональных данных

Пример экзаменационного билета:

Форма 1.4.-33

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Направление 10.03.01 Информационная безопасность

Дисциплина Защита персональных данных

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.
2. Обеспечение защиты информации, в ходе эксплуатации аттестованной ИСПДн.

Зав. Кафедрой УИБ

А.С. Исмагилова

Кафедра управления информационной безопасностью

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

Экзамены:

- 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.

Критерии оценивания результатов экзамена для ОФО:

Критерии оценки (в баллах):

- 25-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание терминологии, основных понятий, умение применять теоретические знания. Студент без затруднений ответил на все дополнительные вопросы.

- 17-24 баллов выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности.

- 10-16 баллов выставляется студенту, если 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 основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос.

- 1-10 баллов выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний. Студент не смог ответить ни на один дополнительный вопрос.

Устный опрос

Устный индивидуальный опрос проводится после изучения новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации.

Модуль 1

Типовые вопросы:

1. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных
2. Нормативное правовое регулирование организации обработки и обеспечения безопасности персональных данных в Российской Федерации

Типовые тестовые задания

При изучении дисциплины используются тестовые задания закрытого типа. Каждое тестовое задание включает вопрос и 4 варианта ответов к нему. Тестирование выполняется в письменной форме.

Необходимо выбрать один ответ из предложенных вариантов.

Модуль 1

1. По признаку отношений к природе возникновения угрозы классифицируются, как:
 - А) Субъективные;
 - Б) Объективные;
 - В) Внешние;
 - Г) Внутренние.
2. «Предоставление информации» это:

А) действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

Б) действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

В) действия, направленные на распространение сведений в средствах массовой информации;

Г) действия, направленные на получение информации как определенным так и неопределенным кругом лиц или передачу информации как определенному так и неопределенному кругу лиц.

3. Специальные категории персональных данных:

А) национальная принадлежность;

Б) состояние интимной жизни;

В) сверхъестественные способности;

Г) Территориальное размещение;

Д) состояние аппетита

Е) политические взгляды.

4. К угрозам непосредственного доступа в операционную среду компьютера, реализуемым в ходе загрузки операционной системы, относятся:

А) реализация DDoS-атак;

Б) анализ сетевого трафика;

В) перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду;

Г) перехват паролей.

5. Наиболее перспективными методами обезличивания ПДн являются:

А) метод подмешивания посторонней информации;

Б) метод декомпозиции;

В) метод разложения;

Г) метод введения идентификаторов;

Д) метод перекомпозиции;

Е) метод варьирования.

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (10 вопросов в варианте)	Неправильный ответ / Правильный ответ	0/1

Типовые темы для дискуссии

Модуль 1

1. Понятие персональных данных работника, общие требования при обработке персональных данных и гарантии их защиты.

2. Принципы обработки персональных данных.

3. Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

4. Организация и обеспечение режимов защиты персональных данных.

Критерии оценки участия в круглом столе (дискуссии)

Показатель оценки	Распределение баллов
Знание и понимание современных тенденций развития системы	1

муниципального управления	
Глубина и оригинальность суждений	1
Аргументированность и взвешенность при изложении своей позиции	1
Умение вести научную дискуссию	1
Активность в обсуждении	1
Соблюдение деловой этики и этикета	1
ИТОГО	6

Типовые задания для контрольной работы

Цель проведения контрольной работы – оценка уровня владения базовой профессиональной терминологией в сфере государственного и муниципального управления. Контрольная работа проводится в письменной форме.

Примеры заданий

Модуль 2

1. Какие обязанности возлагаются на сотрудника, назначаемого ответственным за организацию обработки персональных данных?
2. В каких случаях оператор вправе осуществлять обработку персональных данных без уведомления уполномоченного органа по защите прав субъектов персональных данных?
3. Какие сведения о субъекте относятся к специальным категориям персональных данных?
4. В течение, какого срока, после получения запроса, оператор обязан сообщить субъекту информацию о его персональных данных?
5. В течение, какого срока, оператор обязан внести изменения о персональных данных, являющихся неполными, неточными или неактуальными?

Критерии оценки контрольных работ:

Структура работы	Критерии оценки	Распределение баллов
Один вопрос контрольной работы (в контрольной работе 5 терминов)	Нет ответа / Неполный ответ / Полный ответ	0/2/4

Устный индивидуальный опрос

Устный индивидуальный опрос проводится после изучения новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации.

Модуль 2

Типовые вопросы:

1. Содержание и основные положения Федерального закона «О персональных данных»
2. Меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами
3. Организация работ и назначение ответственных лиц.

Критерии оценки самостоятельной работы:

Структура работы	Критерии оценки	Распределение баллов
Одно задание	Нет ответа / Неполный ответ / Полный ответ с допущением неточностей/ Полный ответ	0/1/2/3

Самостоятельная работа

Модуль 2

Пособия

Основные положения Федерального закона от 27 июля 2006 г. № ФЗ-152 «О персональных данных»

1. Какие обязанности возлагаются на сотрудника, назначаемого ответственным за организацию обработки персональных данных?

2. В каких случаях оператор вправе осуществлять обработку персональных данных без уведомления уполномоченного органа по защите прав субъектов персональных данных?

3. Какие сведения о субъекте относятся к специальным категориям персональных данных?

Критерии оценки самостоятельной работы:

Структура работы	Критерии оценки	Распределение баллов
Одно задание (всего 1 заданий)	Нет ответа / Неполный ответ / Полный ответ	0/5/10

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Степанов-Егиянц, В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации [Электронный ресурс] : монография / В.Г. Степанов-Егиянц. — Электрон. дан. — Москва : СТАТУТ, 2016. — 190 с. — Режим доступа: <https://e.lanbook.com/book/92503>. — Загл. с экрана.
2. Петренко, В.И. Защита персональных данных в информационных системах. Практикум [Электронный ресурс] : учебное пособие / В.И. Петренко, И.В. Мандрица. — Электрон. дан. — Санкт-Петербург : Лань, 2019. — 108 с. — Режим доступа: <https://e.lanbook.com/book/111916>. — Загл. с экрана.

Дополнительная литература

3. Савельев, А.И. Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (постатейный) [Электронный ресурс] / А.И. Савельев. — Электрон. дан. — Москва : СТАТУТ, 2015. — 320 с. — Режим доступа: <https://e.lanbook.com/book/75062>. — Загл. с экрана.
4. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - Москва : Горячая линия-Телеком, 2015. - 585 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0424-8 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=457143>

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/> – 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. 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
<p>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).</p> <p>2. учебная аудитория для проведения лабораторных работ: компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус), Лаборатория систем и сетей передачи данных,</p>	<p>Лекции, лабораторные занятия, текущий контроль, промежуточная аттестация</p>	<p style="text-align: center;">Аудитория № 403</p> <p>Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия.</p> <p style="text-align: center;">Аудитория № 405</p> <p>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. , Настольный 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.</p> <p style="text-align: center;">Аудитория № 413</p> <p>Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p style="text-align: center;">Аудитория № 415</p> <p>Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p style="text-align: center;">Аудитория № 416</p> <p>Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.</p>

<p>сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности аудитория №507 (гуманитарный корпус).</p> <p>3. учебная аудитория для проведения занятий семинарского типа:</p> <p>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).</p> <p>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 (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).</p> <p>5. учебная аудитория для текущего контроля и промежуточной аттестации: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус),</p>	<p>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.</p> <p>Аудитория № 419 Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт.</p> <p>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 SMPRO 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 попитром.</p> <p>Аудитория № 516 Учебная мебель, доска, кресла секционные последующих рядов с попитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.</p> <p>Аудитория № 509 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 608 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 609 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 610 Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDM(m)ver14,10м.</p> <p>Аудитория № 613 Учебная мебель, доска, моноблок стационарный – 15 шт.</p> <p>Компьютерный класс аудитория № 420 Учебная мебель, моноблоки стационарные 15 шт.</p> <p>Компьютерный класс аудитория № 404 Учебная мебель, компьютеры -15 штук.</p> <p>Аудитория 402 читальный зал библиотеки Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные.</p> <p>Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507 Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технические средства обработки информации, стенд "Устройство ПК".</p> <p>Аудитория № 523 Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.</p> <ol style="list-style-type: none"> 1. Windows 8 Russian Russian OLP NL AcademicEdition. 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.
--	---

<p> 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). </p> <p> 6. помещения для самостоятельной работы: читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). </p> <p> 7.помещение для хранения и профилактического обслуживания учебного оборудования: аудитория № 523(гуманитарный корпус). </p>		
---	--	--

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 Защита персональных данных
на 7 семестр

Вид работы	Объем дисциплины
	ОФО
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	37,2
лекций	18
практических/ семинарских	18
лабораторных	0
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	45
Учебных часов на подготовку к экзамену	25,8

Форма контроля
Экзамен 7 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 / Сем	ЛР	СР			
1	2	3	4	5	6	7	8	9
1	Угрозы утечки информации по техническим каналам, актуальность, классификация ТКУИ. Угрозы несанкционированного доступа к персональным данным, обрабатываемым в информационных системах.	4	0	4	0	1- 3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный опрос, дискуссия, тест
2	Методика определения актуальных угроз безопасности персональных данных при их	5	0	5	0	1- 6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Устный опрос, дискуссия, тест

	обработке ИСПДн. ^в Определение уровня защищенности персональных данных.							
3	Состав и содержание мер по обеспечению безопасности персональных данных. Разработка системы защиты персональных данных. Внедрение системы защиты персональных данных.	4	0	4	22	1- 6	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Контрольная работа, самостоятельная работа, устный индивидуальный опрос
4	Обеспечение ЗИ при выводе из эксплуатации, аттестованной ИСПДн. Контроль за соблюдением законодательства Российской Федерации в области персональных	5	0	5	23	1-3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Контрольная работа, самостоятельная работа, устный индивидуальный опрос

	данных. Ответственность за нарушение законодательства о персональных данных.							
	Всего часов	18	0	18	45			

Приложение 2
Рейтинг-план дисциплины
Защита персональных данных

Направление 10.03.01 Информационная безопасность,
курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1.				
Текущий контроль				
1. Устный опрос	3	5	0	15
2. Дискуссия	5	1	0	5
Рубежный контроль				
Тест	1	10	0	10
Всего		16	0	30
Модуль 2.				
Текущий контроль				
1. Контрольная работа	4	5	0	20
Рубежный контроль				
1. Устный индивидуальный опрос	10	1	0	10
2. Самостоятельная работа	10	1		10
Всего		7	0	40
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2. Публикация научной статьи	4	1	0	4
3. Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10
Итоговый контроль				
1. Экзамен	30	1	0	30