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

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

Согласовано:
Председатель УМК института
_____ / Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита персональных данных

Б1.Б.31.05 (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)
к.х.н. _____ / А.А. Султанова

к.ф.-м.н. _____ / Д.С. Юнусова

Уфа 2020

Составитель: А.А. Султанова, Д.С. Юнусова

Рабочая программа дисциплины актуализирована на заседании кафедры управления информационной безопасностью № 9 от 24.04.2020 г.

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/

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

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	место и роль профессии в системе национальной безопасности РФ	– Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета (ОК-4)	
	политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	– Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1)	
	понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	– Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов (ПК-13)	
	правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	– Способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов (ПК-17)	
	методы и средства правовой защиты государственной тайны и информационной безопасности	– Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности (ПК-19)	
Умения	соблюдать нормы профессиональной этики	– Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и	

		служебного этикета (ОК-4)	
	реализовывать на практике принципы политики безопасности	– Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1)	
	использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	– Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов (ПК-13)	
	выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации	– Способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов (ПК-17)	
	использовать в практической деятельности правовые знания	– Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности (ПК-19)	
Владения (навыки / опыт деятельности)	пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности	– Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета (ОК-4)	
	навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	– Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте	

		информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1)	
	навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	– Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов (ПК-13)	
	навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	– Способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов (ПК-17)	
	навыками обеспечения и соблюдения режима секретности	– Способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности; обеспечивать соблюдение режима секретности (ПК-19)	

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

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

Дисциплина изучается на 5 курсе в 9-10-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 специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере специализации «Технологии защиты информации в правоохранительной сфере»: «Международные и российские акты и стандарты по информационной безопасности», «Системы защиты информации в ведущих зарубежных странах», «Правовая защита 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

ОК-4. Способность выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать: место и роль профессии в системе национальной безопасности РФ	Не знает	Знает место и роль профессии в системе национальной безопасности РФ
Второй этап (уровень)	Уметь: соблюдать нормы профессиональной этики	Не умеет	Умеет соблюдать нормы профессиональной этики
Третий этап (уровень)	Владеть: пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности	Не владеет	Владеет пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению 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: место и роль профессии в системе национальной безопасности РФ	Не знает	В целом знает место и роль профессии в системе национальной безопасности РФ, но испытывает трудности при их описании	Знает место и роль профессии в системе национальной безопасности РФ, но допускает незначительные ошибки при их описании	Знает место и роль профессии в системе национальной безопасности РФ
Второй этап (уровень) Базовый	Уметь: соблюдать нормы профессиональной этики	Не умеет	В целом умеет соблюдать нормы профессиональной этики, но допускает значительные ошибки	Умеет соблюдать нормы профессиональной этики, но допускает незначительные ошибки	Умеет соблюдать нормы профессиональной этики
Третий этап (уровень) Повышенный	Владеть: пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности	Не владеет	В целом владеет пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности, но допускает значительные ошибки	Владеет пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности, но допускает незначительные ошибки	Владеет пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности

ПК-1: Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый	Знать: политики, стратегии и технологии	Не знает	Знает политики, стратегии и технологии

этап (уровень)	информационной безопасности и защиты информации, способы их организации и оптимизации		информационной безопасности и защиты информации, способы их организации и оптимизации
Второй этап (уровень)	Уметь: реализовывать на практике принципы политики безопасности	Не умеет	Умеет реализовывать на практике принципы политики безопасности
Третий этап (уровень)	Владеть: навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	Не владеет	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления

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 допускает значительные ошибки 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	Умеет реализовывать на практике принципы политики безопасности, но допускает незначительные ошибки	Умеет реализовывать 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 испытывает затруднения в условиях конкретной задачи	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-13: Способность осуществлять организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать: понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	Не знает	Знает понятие системы управления, основные виды структур, принципы системного подхода к анализу структур
Второй этап (уровень)	Уметь: использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	Не умеет	Умеет использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности
Третий этап (уровень)	Владеть: навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	Не владеет	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для 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: понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	Не знает	В целом знает понятие системы управления, основные виды структур, принципы системного подхода к анализу структур, но допускает	Знает понятие системы управления, основные виды структур, принципы системного подхода к анализу структур, но	Знает понятие системы управления, основные виды структур, принципы системного подхода к анализу структур

			значительные ошибки	допускает незначительные ошибки	
Второй этап (уровень) Базовый	Уметь: использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности	Не умеет	В целом умеет использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности, но допускает значительные ошибки	Умеет использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности, но допускает незначительные ошибки	Умеет использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по информационной безопасности
Третий этап (уровень) Повышенный	Владеть: навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	Не владеет	В целом владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью, допускает незначительные ошибки	Владеет навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью

ПК-17: Способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать: правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	Не знает	Знает правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации
Второй этап (уровень)	Уметь: выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации	Не умеет	Умеет выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации
Третий этап (уровень)	Владеть: навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Не владеет	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области 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: правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	Не знает	В целом знает правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации, но допускает значительные ошибки	Знает правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации, но допускает незначительные ошибки	Знает правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации
Второй этап (уровень) Базовый	Уметь: выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации	Не умеет	В целом умеет выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации, но допускает значительные ошибки	Умеет выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации, но допускает незначительные ошибки	Умеет выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации

Третий этап (уровень) Повышенный	Владеть: навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Не владеет	В целом владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации, допускает незначительные ошибки	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области 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	
		«Не зачтено»	«Зачтено»
Первый этап (уровень)	Знать: методы и средства правовой защиты государственной тайны и информационной безопасности	Не знает	Знает методы и средства правовой защиты государственной тайны и информационной безопасности
Второй этап (уровень)	Уметь: использовать в практической деятельности правовые знания	Не умеет	Умеет использовать в практической деятельности правовые знания
Третий этап (уровень)	Владеть: навыками обеспечения и соблюдения режима секретности	Не владеет	Владеет навыками обеспечения и соблюдения 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 (уровень) Пороговый	Знать: методы и средства правовой защиты государственной тайны и информационной безопасности	Не знает	В целом знает методы и средства правовой защиты государственной тайны и информационной безопасности, но допускает значительные ошибки	Знает методы и средства правовой защиты государственной тайны и информационной безопасности, но допускает незначительные ошибки	Знает методы и средства правовой защиты государственной тайны и информационной безопасности
Второй этап (уровень) Базовый	Уметь: использовать в практической деятельности правовые знания	Не умеет	В целом умеет использовать в практической деятельности правовые знания, но допускает значительные ошибки	Умеет использовать в практической деятельности правовые знания, но допускает незначительные ошибки	Умеет использовать в практической деятельности правовые знания
Третий этап (уровень) Повышенный	Владеть: навыками обеспечения и соблюдения режима секретности	Не владеет	В целом владеет навыками обеспечения и соблюдения режима секретности	Владеет навыками обеспечения и соблюдения режима секретности, допускает незначительные ошибки	Владеет навыками обеспечения и соблюдения режима секретности

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

Зачет: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10.

Шкалы оценивания для зачета:

• зачтено - от 60 до 110 баллов (включая 10 поощрительных баллов),

• не зачтено — от 0 до 59 баллов.

Экзамен:

- 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.

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	место и роль профессии в системе национальной безопасности РФ	ОК-4	Тест, контрольная работа, практическая работа
	политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	ПК-1	Тест, контрольная работа, практическая работа
	понятие системы управления, основные виды структур, принципы системного подхода к анализу структур	ПК-13	Тест, контрольная работа, практическая работа
	правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	ПК-17	Тест, контрольная работа, практическая работа
	методы и средства правовой защиты государственной тайны и информационной безопасности	ПК-19	Тест, контрольная работа, практическая работа
2-й этап Уметь	соблюдать нормы профессиональной этики	ОК-4	Тест, контрольная работа, практическая работа
	реализовывать на практике принципы политики безопасности	ПК-1	Тест, контрольная работа, практическая работа
	использовать методы количественного представления информации и основные закономерности ее преобразования в каналах при выполнении комплекса мер по	ПК-13	Тест, контрольная работа, практическая работа

	информационной безопасности		
	выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации	ПК-17	Тест, контрольная работа, практическая работа
	использовать в практической деятельности правовые знания	ПК-19	Тест, контрольная работа, практическая работа
3-й этап Владеть	пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности	ОК-4	Тест, контрольная работа, практическая работа
	навыками анализа, обработки и интерпретации результатов решения прикладных задач управления	ПК-1	Тест, контрольная работа, практическая работа
	навыками анализа, обработки и интерпретации результатов решения прикладных задач управления; навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	ПК-13	Тест, контрольная работа, практическая работа
	навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	ПК-17	Тест, контрольная работа, практическая работа
	навыками обеспечения и соблюдения режима секретности	ПК-19	Тест, контрольная работа, практическая работа

Зачет

1. Нормативное правовое регулирование организации обработки и обеспечения безопасности персональных данных в Российской Федерации.

2. Содержание и основные положения Федерального закона «О персональных данных».

3. Меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами.

4. Организация работ и назначение ответственных лиц.

5. Прием и обработка обращений и запросов субъектов персональных данных или их представителей.

6. Обследование информационных систем организации и описание процессов обработки персональных данных.

7. Особенности обработки биометрических персональных данных.

8. Определение перечня информационных систем персональных данных и перечня должностей сотрудников, допущенных к обработке персональных данных в организации.

9. Политика в отношении обработки персональных данных в организации.

10. Согласие на обработку персональных данных.

11. Ознакомление работников с порядком обработки и обеспечения безопасности персональных данных.

12. Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных.

13. Организация обработки персональных данных, осуществляемой без средств автоматизации.

14. Требования и методы по обезличиванию персональных данных.

15. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

16. Разработка уведомления об обработке (о намерении осуществлять обработку) персональных данных.

17. Осуществление внутреннего контроля соответствия обработки персональных данных установленным требованиям.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей, перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкала оценивания для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

Экзамен

Структура экзаменационного билета

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

Типовые экзаменационные материалы

1. Нормативное правовое регулирование организации обработки и обеспечения безопасности персональных данных в Российской Федерации.

2. Содержание и основные положения Федерального закона «О персональных данных».

3. Меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами.

4. Организация работ и назначение ответственных лиц.

5. Прием и обработка обращений и запросов субъектов персональных данных или их представителей.

6. Обследование информационных систем организации и описание процессов обработки персональных данных.

7. Особенности обработки биометрических персональных данных.

8. Определение перечня информационных систем персональных данных и перечня должностей сотрудников, допущенных к обработке персональных данных в организации.

9. Политика в отношении обработки персональных данных в организации.

10. Согласие на обработку персональных данных.

11. Ознакомление работников с порядком обработки и обеспечения безопасности персональных данных.

12. Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных.

13. Организация обработки персональных данных, осуществляемой без средств автоматизации.

14. Требования и методы по обезличиванию персональных данных.

15. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

16. Разработка уведомления об обработке (о намерении осуществлять обработку) персональных данных.

17. Осуществление внутреннего контроля соответствия обработки персональных данных установленным требованиям.

18. Принятие правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке.

19. Формирование требований к системе защиты персональных данных.

20. Угрозы утечки информации по техническим каналам, актуальность, классификация ТКУИ.

21. Угрозы несанкционированного доступа к персональным данным, обрабатываемым в информационных системах.

22. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационной системе персональных данных.

23. Определение уровня защищённости персональных данных.

24. Состав и содержание мер по обеспечению безопасности персональных данных.

25. Разработка системы защиты персональных данных.

26. Внедрение системы защиты персональных данных.

27. Состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации.

28. Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных.

29. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы персональных данных.

30. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы персональных данных.

31. Контроль за соблюдением законодательства Российской Федерации в области персональных данных.

32. 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

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Дисциплина Защита персональных данных

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Нормативное правовое регулирование организации обработки и обеспечения безопасности персональных данных в Российской Федерации.
2. Принятие правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке.

Зав. Кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

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 при выполнении практических заданий. 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 при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.

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.

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 (Семестр 9, 10)

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 (семестр 9: 10 вопросов в варианте; семестр 10: 20 вопросов)	Неправильный ответ / Правильный ответ	0/1

Типовые задания для контрольной работы

Цель проведения контрольной работы – оценка уровня владения базовой профессиональной терминологией. Контрольная работа проводится в письменной форме.

Примеры заданий

Модуль 2 (Семестр 9, 10)

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	Нет ответа / Неполный ответ / Полный ответ	0/5/10

Практические работы

Модуль 1, 2 (Семестр 9, 10)

Проводится в виде дискуссии

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. Какие обязанности возлагаются на сотрудника, назначаемого ответственным за организацию обработки персональных данных?
4. В каких случаях оператор вправе осуществлять обработку персональных данных без уведомления уполномоченного органа по защите прав субъектов персональных данных?
5. Какие сведения о субъекте относятся к специальным категориям персональных данных?
6. Понятие персональных данных работника, общие требования при обработке персональных данных и гарантии их защиты.
7. Принципы обработки персональных данных.
8. Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
9. Организация и обеспечение режимов защиты персональных данных.

Критерии оценки работы:

Структура работы	Критерии оценки	Распределение баллов
Одно задание (всего 1 заданий)	Нет ответа / участие в дискуссии / подготовка доклада	0/10/20

4.3. Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 2.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для

освоения дисциплины

Основная литература

1. Системы инженерно-технической защиты информации [Электронный ресурс]. Ч.1: методические издания / Башкирский государственный университет ; сост. И.В. Салов; А.С. Исмагилова. — Уфа: РИЦ БашГУ, 2018. — Электрон. версия печ. публикации. — Доступ возможен через Электронную библиотеку БашГУ. — <URL:https://elib.bashedu.ru/dl/local/Salov_Ismagilova_sost_Sistemy ITZI_ch 1_mu_2018.pdf>.

2. Системы инженерно-технической защиты информации [Электронный ресурс]. Ч.2: методические указания / Башкирский государственный университет ; сост. И.В. Салов; А.С. Исмагилова. — Уфа: РИЦ БашГУ, 2018. — Электрон. версия печ. публикации. — Доступ возможен через Электронную библиотеку БашГУ. — <URL:https://elib.bashedu.ru/dl/local/Salov_Ismagilova_sost_Sistemy ITZI_ch 2_mu_2018.pdf>.

3. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учебное пособие / В.Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578.

Дополнительная литература

4. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. - 222 с. : ил. - Библиогр.: с. 214-215. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458204 .

5. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93245

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

1. Management. Учебно-методический комплекс – http://bgumanagement2009.narod.ru
2. Научная электронная библиотека https://elibrary.ru
3. Информационно-коммуникационные технологии в образовании http://www.ict.edu.ru/
4. ФСБ России http://fsb.ru
5. ФСТЭК http://fstec.ru
6. Консультант плюс http://www.consultant.ru/

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),	Лекции, практические занятия, 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

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), 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		RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 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 № 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.

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).		**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 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 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Защита персональных данных на 9 семестр
ОФО

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	72,2
лекций	36
практических/ семинарских	36
лабораторных	0
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	36
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	0

Форма контроля:
Зачет 9 семестр

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Защита персональных данных на 10 семестр
ОФО

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	5 ЗЕТ / 180 часов
Учебных часов на контактную работу с преподавателем:	49,2
лекций	16
практических/ семинарских	32
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)	78
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	52,8

Форма контроля
Экзамен 10 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
Модуль 1								
1	Актуальность. Основные понятия и определения	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
2	Основные положения ФЗ-152 «О персональных данных»	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
3	Меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренны	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа

	х 152-ФЗ и принятых в соответствии с ним нормативными правовыми актами							
4	Организация работ и назначение ответственных лиц	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
5	Особенности обработки биометрических персональных данных	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
6	Определение перечня информационных систем персональных данных и перечня должностей сотрудников, допущенных к обработке персональных	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа

	данных в организации							
7	Политика в отношении обработки персональных данных в организации	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
8	Согласие на обработку персональных данных	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
9	Ознакомление работников с порядком обработки и обеспечения безопасности персональных данных. Порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа

Модуль 2								
10	Организация обработки персональных данных, осуществляемой без средств автоматизации	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Контрольная работа, практическая работа
11	Требования и методы по обезличиванию персональных данных	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
12	Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне ИСПДн	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
13	Разработка уведомления об обработке (о намерении осуществлять обработку)	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа

	персональных данных							
14	Осуществление внутреннего контроля соответствия обработки персональных данных установленным требованиям	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
15	Принятие правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
16	Формирование требований к системе защиты персональных данных Оценка вреда, который может быть причинён субъектам персональных	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа

	данных							
17	Угрозы утечки информации по техническим каналам, актуальность, классификация ТКУИ	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
18	Угрозы несанкционированного доступа к персональным данным, обрабатываемым в информационных системах	2	2	0	2	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
	Всего часов	36	36	0	36			

№	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
Модуль 1								
19	Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн	2	4	0	10	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
20	Определение уровня защищенности персональных данных	2	4	0	10	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
21	Состав и содержание мер по обеспечению безопасности	2	4	0	10	1- 7	Самостоятельное изучение рекомендуемой основной и	Тест, практическая работа

	персональных данных						дополнительной литературы	
22	Разработка и внедрение системы защиты персональных данных	2	4	0	10	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
Модуль 2								
23	Состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации	2	4	0	10	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Контрольная работа, практическая работа
24	Обеспечение защиты информации в ходе и при выводе из эксплуатации	2	4	0	10	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной	Тест, практическая работа

	аттестованной ИСПДн						литературы	
25	Контроль за соблюдением законодательства Российской Федерации в области персональных данных	2	4	0	10	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
26	Ответственность за нарушение законодательства о персональных данных	2	4	0	8	1- 7	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
	Всего часов	16	32	0	78			

Приложение 2

Рейтинг-план дисциплины

Защита персональных данных

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере курс 5, семестр

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1.				
Текущий контроль				
1. Практическая работа	20	2	0	40
Рубежный контроль				
Тест	10	1	0	10
Всего		3	0	50
Модуль 2.				
Текущий контроль				
1. Контрольная работа	10	1	0	10
Рубежный контроль				
1. Практическая работа	20	2	0	40
Всего		3	0	50
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. Зачет				
Итого				110

Рейтинг-план дисциплины

Защита персональных данных

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере курс 5, семестр 10

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1.				
Текущий контроль				
Практическая работа	20	1	0	20
Рубежный контроль				
Контрольная работа	10	1	0	10
Всего		2	0	30
Модуль 2.				
Текущий контроль				
Тест	20	1	0	20
Рубежный контроль				
Практическая работа	20	1	0	20
Всего		2	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