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

Актуализировано:
на заседании кафедры
протокол от «07» июня 2018 г. № 10
Зав. кафедрой /А.С. Исмагилова

Согласовано:
Председатель УМК института
/Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита и обработка конфиденциальных документов
Б1.Б.28 (базовая)

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации

Квалификация
бакалавр

Разработчик (составитель)
к.филос.н., доцент /Н.Г. Миронова

Для приема: 2015 г.

Уфа 2018 г.

Составитель: Н.Г.Миронова

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

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

Заведующий кафедрой _____/ _____Ф.И.О/

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

Заведующий кафедрой _____/ _____Ф.И.О/

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

Заведующий кафедрой _____/ _____Ф.И.О/

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

Заведующий кафедрой _____/ _____Ф.И.О/

Список документов и материалов

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

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	Знать место и роль профессии в системе национальной безопасности РФ Знать социальные ценности общества и их связь с социальной значимостью своей будущей профессии Знать основные виды социальных организаций и способы взаимодействия в них Знать основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета	ОК-5. Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.	
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации Знать общеметодологические принципы теории информационной безопасности Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации Знать состояние законодательной базы и стандарты в области информационной безопасности	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации Знать общеметодологические принципы теории информационной безопасности Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации Знать состояние законодательной базы и стандарты в области информационной безопасности	ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
	Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации Знать также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области Знать методы и средства правовой защиты государственной тайны и информационной	ПК-15. Способность 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	

	безопасности	техническому и экспортному контролю	
Умения	Уметь осознавать социальную значимость своей профессии, Уметь находить баланс между интересами личности, общества и государства Уметь соблюдать нормы профессиональной этики	ОК-5. Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.	
	Уметь реализовывать на практике принципы политики безопасности; Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности Уметь обосновывать организационно-технические мероприятия по защите информации Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
	Уметь реализовывать на практике принципы политики безопасности; Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности Уметь обосновывать организационно-технические мероприятия по защите информации Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
	Уметь использовать в практической деятельности правовые знания Уметь анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности Уметь предвидеть юридические опасности и угрозы и соблюдать основные правовые требования информационной безопасности, в т.ч. для защиты государственной тайны	ПК-15. Способность 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	
Навыки, опыт дея-	Владеть пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности	ОК-5. Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к	

тельности	Владеть навыками творческого мышления для выполнения профессиональных задач в области обеспечения безопасности информационных технологий и защиты интересов личности, общества и государства	выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.	
	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации Владеть навыками выявления и устранения угроз информационной безопасности Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий Владеть навыками внедрения, адаптации и настройки средств защиты прикладных ИС	ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации Владеть навыками выявления и устранения угроз информационной безопасности Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий	ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
	Владеть основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации Владеть навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности Владеть навыками поиска нормативной правовой информации необходимой для профессиональной деятельности Владеть навыками обеспечения и соблю-	ПК-15. Способность 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	

	дения режима секретности		

2. Цели и место дисциплины в структуре образовательной программы

Дисциплина «Защита и обработка конфиденциальных документов» относится к группе дисциплин базовой части образовательной программы, изучается в 6,7 семестрах на 3,4 курсах.

Цели освоения дисциплины: приобрести знания о мероприятиях по обеспечению информационной безопасности при ведении защищенного документооборота, комплекса мероприятий по защите информации в процессах автоматизированной обработки информации, навыки организации конфиденциального документооборота и делопроизводства, создания и обработки служебных документов, навыки работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, навыками обеспечения и соблюдения режима секретности.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин, которые направлены на формирование компетенций ОК-5; ПК-4; ПК-13; ПК-15: Защита коммерческой тайны , Защита персональных данных, История, Кадровая безопасность на предприятии, Комплексная система защиты информации на предприятии , Криптографические методы защиты информации, Международные и российские нормативные акты и стандарты по информационной безопасности, Организационное и правовое обеспечение информационной безопасности, Организация и управление службой защиты информации , Основы информационной безопасности , Правовая защита профессиональной тайны, Правовая охрана результатов интеллектуальной деятельности, Программно-аппаратные средства защиты информации, Социология, Структура и основы деятельности предприятий различных форм собственности, Техническая защита информации, Управление персоналом, Функциональный процесс и организация предприятия, Экономика 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

ОК-5. Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.

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	Знать место и роль профессии в системе национальной безопасности РФ Знать социальные ценности общества и их связь с социальной значимостью своей будущей профессии Знать основные виды социальных организаций и способы взаимодействия в них Знать основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета	Не знает	Слабо знает указанные понятия, способы и принципы.	Демонстрирует хорошее знание указанных понятий, способов и принципов, но не всегда способен увязать их с практикой управления службой защиты информации.	Демонстрирует целостные, системные знания в указанной сфере.
Второй этап	Уметь осознавать социальную значимость своей профессии, Уметь находить баланс между интересами личности, общества и государства Уметь соблюдать нормы профессиональной этики	Не умеет	Слабо демонстрирует указанные умения и знания, без связи с практическими навыками	Демонстрирует хорошее теоретическое знание компетенции, но недостаточное владение практической стороной при решении задач работы с документами	Демонстрирует уверенное, свободное владение указанными навыками при решении задач работы с документами
Третий этап	Владеть пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности Владеть навыками творческого мышления для выполнения профессиональных задач в области обеспечения безопасности информационных технологий и защиты интересов личности, общества и государства	Не владеет	Слабо демонстрирует указанные навыки.	Демонстрирует хорошее владение компетенцией, но имеет устаревшие и малоактуальные сведения.	Демонстрирует уверенное, свободное владение указанными навыками при решении задач работы с документами

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

Этап (уровень) освоения компе-	Планируемые результаты обучения (показатели достижения заданного уровня освое-	Критерии оценивания результатов обучения			
		2 («Не удовле- твори-	3 («Удов- («Удов- летвори-	4 («Хорошо»)	5 («Отлично»)

тенции	ния компетенций)	тельно»)	тельно»)		
Первый этап	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации Знать общеметодологические принципы теории информационной безопасности Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации Знать состояние законодательной базы и стандарты в области информационной безопасности	Не знает	Демонстрирует фрагментарные знания.	Демонстрирует хорошее знание, но с трудом ориентируется в них при решении практических задач или знание - несколько устаревшее, утратившее актуальность.	Демонстрирует целостные, системные знания в указанной сфере, свободно ориентируется в них при решении практических задач.
Второй этап	Уметь реализовывать на практике принципы политики безопасности; Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности Уметь обосновывать организационно-технические мероприятия по защите информации Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	Не умеет	Слабо демонстрирует указанные умения и знания, без связи навыками решения задач работы с документами.	Демонстрирует хорошее теоретическое знание компетенции, но недостаточное владение практической стороной при решении задач работы с документами	Демонстрирует уверенное, свободное владение указанными навыками при решении задач работы с документами
Третий этап	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информаци-	Не владеет	Слабо демонстрирует указанные навыки.	Демонстрирует хорошее владение компетенции, но в полной мере или имеет устаревшие сведения	Демонстрирует уверенное, свободное владение указанными навыками при решении задач работы с документами

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

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

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации Знать общеметодологические принципы теории информационной безопасности Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации Знать состояние законодательной базы и стандарты в области информационной безопасности	Не демонстрирует указанных знаний	Демонстрирует фрагментарные знания.	Демонстрирует хорошее знание, но с трудом ориентируется в них при решении практических задач или знание - несколько устаревшее, утратившее актуальность.	Демонстрирует целостные, системные знания в указанной сфере, свободно ориентируется в них при решении профессиональных задач.

Второй этап	Уметь реализовывать на практике принципы политики безопасности; Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности Уметь обосновывать организационно-технические мероприятия по защите информации Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации	Не умеет	Слабо демонстрирует указанные умения и знания, без связи навыками решения профессиональных задач	Демонстрирует хорошее теоретическое знание компетенции, но недостаточное владение практической стороной при решении профессиональных задач.	Демонстрирует уверенное, свободное владение указанными навыками при решении профессиональных задач
Третий этап	Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации Владеть навыками выявления и устранения угроз информационной безопасности Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий	Не владеет и не имеет теоретических знаний об этой сфере	Слабо демонстрирует указанные навыки и знания.	Демонстрирует хорошее владение компетенцией, но имеет устаревшие сведения.	Демонстрирует уверенное, свободное владение указанными навыками при решении профессиональных задач

ПК-15. Способность 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 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап	Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации Знать также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области Знать методы и средства правовой защиты государственной тайны и информационной безопасности	Не знает	Слабо знает указанные понятия, способы и принципы.	Демонстрирует хорошее знание понятий, способов и принципов, но не всегда способен увязать их с практикой работы с документами	Демонстрирует целостные, системные знания в указанной сфере.
Второй этап	Уметь использовать в практической деятельности правовые знания Уметь анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности Уметь предвидеть юридические опасности и угрозы и соблюдать основные правовые требования информационной безопасности, в т.ч. для защиты государственной тайны	Не умеет	Слабо демонстрирует указанные умения и знания, без связи навыками решения профессиональных задач	Демонстрирует хорошее теоретическое знание компетенции, но недостаточное владение практической стороной работы с документами	Демонстрирует уверенное, свободное владение указанными навыками при решении профессиональных задач.

Третий этап	Владеть основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации Владеть навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности Владеть навыками поиска нормативной правовой информации необходимой для профессиональной деятельности Владеть навыками обеспечения и соблюдения режима секретности	Не владеет	Слабо демонстрирует указанные навыки.	Демонстрирует хорошее владение компетенцией, но имеет устаревшие сведения.	Демонстрирует уверенное, свободное владение указанными навыками при работе с документами

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

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1-й этап Знания	Знать место и роль профессии в системе национальной безопасности РФ Знать социальные ценности общества и их связь с социальной значимостью своей будущей профессии Знать основные виды социальных организаций и способы взаимодействия в них Знать основные задачи своей профессии в соответствии с нормами морали, профессиональной этики и служебного этикета Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации Знать общеметодологические принципы теории информационной безопасности Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации Знать состояние законодательной базы и стандарты в области информационной безопасности Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации Знать общеметодологические принципы теории информационной безопасности Знать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации Знать состояние законодательной базы и стандарты в	ОК-5. Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики. ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации ПК-15. Способность 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	Устный опрос, тестирование, практическое задание, доклад семинара, контрольная самостоятельная работа

	области информационной безопасности Знать основные нормативные и правовые акты в области информационной безопасности и защиты информации Знать также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области Знать методы и средства правовой защиты государственной тайны и информационной безопасности		
2-й этап Умения	Уметь осознавать социальную значимость своей профессии, Уметь находить баланс между интересами личности, общества и государства Уметь соблюдать нормы профессиональной этики Уметь реализовывать на практике принципы политики безопасности; Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности Уметь обосновывать организационно-технические мероприятия по защите информации Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации Уметь реализовывать на практике принципы политики безопасности; Уметь использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной безопасности Уметь обосновывать организационно-технические мероприятия по защите ин-	ОК-5. Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики. ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации ПК-15. Способность 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	Устный опрос, тестирование, практическое задание, доклад семинара, контрольная самостоятельная работа

	формации Уметь использовать возможности и особенности организационных, аппаратных и программных средств безопасности и защиты информации Уметь использовать в практической деятельности правовые знания Уметь анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности Уметь предвидеть юридические опасности и угрозы и соблюдать основные правовые требования информационной безопасности, в т.ч. для защиты государственной тайны		
3-й этап владение навыками	Владеть пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности Владеть навыками творческого мышления для выполнения профессиональных задач в области обеспечения безопасности информационных технологий и защиты интересов личности, общества и государства Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизирован-	ОК-5. Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики. ПК-4. Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты ПК-13. Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации ПК-15. Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федераль-	Устный опрос, тестирование, практическое задание, доклад семинара, контрольная самостоятельная работа

	ной обработки информации Владеть навыками выявления и устранения угроз информационной безопасности Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий Владеть навыками внедрения, адаптации и настройки средств защиты прикладных ИС Владеть навыками анализа, обработки и интерпретации результатов решения прикладных задач управления Владеть навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью Владеть навыками организации комплекса мероприятий по защите информации в процессах автоматизированной обработки информации Владеть навыками выявления и устранения угроз информационной безопасности Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий Владеть основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации Владеть навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности Владеть навыками поиска нормативной правовой информации необходимой для профессиональной деятельности Владеть навыками обеспе-	ной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	

	чения и соблюдения режима секретности		

4.3. Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в Приложении 2.

Экзамен

Структура экзаменационного билета.

Экзаменационный билет содержит 2 теоретических вопроса.

Типовые экзаменационные вопросы:

1. Правовые акты и законы, регулирующие защиту конфиденциальной информации (и дать краткую характеристику содержанию законов, регулирующих обращение с конфиденциальной информацией).
2. Виды конфиденциальной информации.
3. Угрозы конфиденциальной информации.
4. Обзор организационных и технических мер обеспечения безопасности информации, содержащейся в электронных и бумажных конфиденциальных документах.
5. Организация конфиденциального делопроизводства.
6. Функции подразделения конфиденциального делопроизводства.
7. Перечни конфиденциальных сведений.
8. Понятие конфиденциального делопроизводства. Перечни конфиденциальных документов.
9. Система доступа к конфиденциальным документам.
10. Учет носителей конфиденциальной информации. Учет издаваемых конфиденциальных документов.
11. Получение конфиденциальных документов и их учет.
12. Отправление конфиденциальных документов.
13. Порядок копирования конфиденциальных документов.
14. Организация исполнения конфиденциальных документов.
15. Номенклатура конфиденциальных дел. Формирование конфиденциальных дел. Оформление конфиденциальных дел.
16. Подготовка конфиденциальных дел и документов для архивного хранения.
17. Требования к помещениям подразделения конфиденциального делопроизводства. Передача помещений конфиденциального делопроизводства под охрану.
18. Порядок обращения с конфиденциальными документами.
19. Контроль наличия конфиденциальных документов.
20. Подготовка к проведению конфиденциальных совещаний. Порядок проведения конфиденциальных совещаний.
21. Проведение внутренних расследований по фактам утраты конфиденциальных документов или разглашения конфиденциальной информации.
22. Особенности защиты информации в системах электронного документооборота. Понятие и формы реализации защищенного электронного документооборота.
23. Экспертиза конфиденциальных документов. Экспертная комиссия и порядок ее работы при передачи документов на хранение в архив или уничтожение.
24. Порядок уничтожения и архивного хранения конфиденциальных документов, порядок снятия грифа конфиденциальности.
25. Ответственность за разглашение информации, содержащейся в конфиденциальных документах разной степени конфиденциальности.
26. Криптозащита (шифрование) как мера зашиты КИ.

Образец экзаменационного билета:

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

Направление подготовки **10.03.01 Информационная безопасность**

Дисциплина **Защита и обработка конфиденциальных документов**

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 18

1. Порядок обращения с конфиденциальными документами.
2. Криптозащита (шифрование) как мера защиты КИ.

Зав. кафедрой УИБ А.С. Исмагилова

2018-2019 учебный год
Кафедра управления информационной безопасностью

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

25-30 баллов

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

17-24 баллов

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

10-16 баллов

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

1-9 баллов

Ответ на теоретический вопрос свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Студент не смог ответить ни на один дополнительный вопрос. При этом студент не решил задачу или лишь частично (на ½ от задания).

Перевод оценки из 100-балльной в 4-балльную производится следующим образом:
- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов);
- хорошо – от 60 до 79 баллов;
- удовлетворительно – от 45 до 59 баллов;
- неудовлетворительно – менее 45 баллов.

Типовые вопросы устных опросов

Устный индивидуальный опрос проводится после изучения новой темы, во время практического занятия, с целью выяснения наиболее сложных вопросов, степени усвоения информации. Студент излагает содержание вопроса изученной темы, либо отвечает на поставленный устный вопрос, предварительно (домашняя работа) ознакомившись с материалами лекции и дополнительной литературы.

Примерные вопросы для опроса:

1. Правовое обеспечение информационной безопасности.
2. Российские документы по защите информации.
3. Организационное обеспечение информационной безопасности
4. Законодательные и нормативные акты РФ в области защиты информации.
5. Найдите документы, определяющие правила и нормативы обработки и хранения КД
6. Сравнительный анализ системы защиты конфиденциальных документов в РФ и США
7. Подготовка конфиденциальных дел и документов для архивного хранения
8. Экспертиза ценности документа
9. Понятие документа
10. Понятие конфиденциального документооборота
11. Экспедиционная обработка исходящих конфиденциальных документов.
12. Организация и контроль исполнения конфиденциальных документов.
13. Правила работы исполнителя
14. Перечень конфиденциальных сведений
15. Перечень конфиденциальных документов, методика их формирования
16. Правила формирования и оформления конфиденциальных дел
17. Учет конфиденциальных документов
18. Уничтожение конфиденциальных документов
19. Этапы проведения служебного расследование по факту утери конфиденциального документа
20. Понятие и виды конфиденциальной информации в современном российском законодательстве
21. Особенности оформления реквизитов конфиденциальных документов
22. Правила издания, копирования и тиражирования конфиденциальных документов
23. Законодательная база защиты документированной информации в РФ
24. Подзаконные нормативно-правовые акты в сфере защиты информации
25. Определение требований к защите и категорирование ресурсов.
26. Проведение обследования компьютерной сети, инвентаризация, категорирование и документирование защищаемых ресурсов автоматизированных систем.
27. Оценка политик безопасности
28. Рекомендации по тестированию.
29. Цель, методы и порядок проведения тестирования.
30. Проверка реальных условий размещения и использования оборудования.
31. Тестовые испытания функций защиты от НСД и защиты от утечки по техническим каналам.

32. Моделирование действий злоумышленника (―взлом‖ защиты информации).

Критерии и методика оценивания результата устного опроса.

Студент может быть опрошен неоднократно (до 5 раз) в течении семестра, за каждый ответ на один из вышеприведенных вопросов по проверке усвоения компетенции может начислено до 3 балла за правильный ответ.

Комплект типовых практических заданий

Студент может выступить на семинаре с докладом по перечню тем докладов теоретической части (или участвовать в устном опросе), а затем выполнить задания практической части.

Модуль 1.

Практическое занятие 1. Основные понятия курса «Защита и обработка конфиденциальных документов»

Теоретическая часть

Темы докладов:

1. Цели и объекты защиты конфиденциальной информации.
2. Виды конфиденциальной информации. Понятие государственной и профессиональной тайны.
3. Потенциальные угрозы (и злоумышленники) конфиденциальной информации. Каналы утечки конфиденциальной информации.
4. Способы, средства, методы защиты конфиденциальной информации.
5. Устный опрос.

Практическое занятие 2,3. Нормативная база, регулирующая обработку конфиденциальной и секретной информации

Теоретическая часть:

1. Законы и правовые нормы, регулирующие работу с конфиденциальной информацией,
2. Законы и правовые нормы, регулирующие работу с документами, содержащими государственную тайну.
3. Правовые основы защищенного документооборота.
4. Понятие защищенного документооборота. Основные задачи конфиденциального делопроизводства.
5. Потенциальные опасности и проблемы информационной безопасности конфиденциальных электронных данных при обработке их программами, с использованием цифровой техники.
6. Средства и меры безопасности при работе с оцифрованными документами и цифровыми данными.

Практическое задание на ознакомление с содержанием законов о служебной тайне, коммерческой тайне, гос.тайне, о персональных данных и т.д., постановлений правительства, приказов регулирующих органов (ФСТЭК, ФСБ) в части мер по обеспечении защиты информации, содержащихся в документах.

Практическое занятие 4,5. Движение, реквизиты конфиденциальных документов.

Теоретическая часть:

1. Документопотоки: входящий, издаваемый, выделенного хранения.
2. Состав технологических этапов и операций.
3. Сущность задачи и особенности конфиденциального делопроизводства.
4. Отправление конфиденциальных документов.
5. Общие требования к учету конфиденциальных документов.
6. Понятие, категории конфиденциальных документов. Перечень конфиденциальных сведений.
7. Грифы и сроки конфиденциальности документов. Степень конфиденциальности. Система доступа к конфиденциальным документам.
   Практическая часть: оформление документов по заданиям.

Модуль 2.

Практическое занятие 6,7. Учет конфиденциальных документов.

Теоретическая часть:
Система доступа к конфиденциальным документам. Принципы распределения документов между руководителями, структурными подразделениями и специалистами. Уровень компетенции должностных лиц решении вопросов, поставленных в документах.

1. Учет носителей конфиденциальной информации. Журналы или картотеки учета изданных и поступивших документов.
2. Учет поступивших конфиденциальных документов.
3. Учет изданных конфиденциальных документов.
4. Учет конфиденциальных документов выделенного хранения.
5. Учет изданных конфиденциальных распорядительных документов и протоколов. Журнал
6. Копирование и размножение конфиденциальных документов.
7. Устный опрос.

Практическое занятие 8. Оперативное хранение конфиденциальных документов.

Теоретическая часть:

1. Номенклатура дел организации и ее разделы (Заполнение граф номенклатуры дел на конкретном примере). Номенклатура конфиденциальных дел.
2. Формирование и оформление конфиденциальных дел.
3. Дело. Опись документов дела. Карточка учета выдачи дела. Заверительная надпись дела.
4. Дополнительные требования к формированию в дела конфиденциальных документов. Нумерация листов.
5. Оформление карточки учета выдачи дела.
6. Формирование и хранение дел, содержащих конфиденциальные документы.
7. Оперативное хранение конфиденциальных документов – основные требования.
8. Устный опрос.

Модуль 3. 7 семестр

Практическое занятие 9. Учет, движение, проверка наличия конфиденциальных документов.

Теоретическая часть.
Темы докладов:

1. Назначение и задачи проверки наличия документов, дел и носителей информации.
2. Сферы распространения проверки.
3. Требования, предъявляемые к проверке.
4. Виды и периодичность проверок наличия и уровень конфиденциальности информации.
5. Типовой состав процедур и операций проверки наличия.
6. Текущая проверка наличия документов, дел и носителей информации. Ее цели, состав проверяемых документов.
7. Оформление результата проверки конфиденциальных документов.
8. Проверка наличия документов, дел и носителей информации при увольнении сотрудника.
9. Порядок приема от увольняющегося документов, дел и носителей информации.
10. Проверка наличия и сохранности баз данных в ЭВМ.
11. Оформление результата проверки.
12. Предпосылки нерегламентированных проверок наличия документов, дел и носителей информации.
13. Цели проверки, состав проверяемых документов и оформление результата проверки.

Практическое занятие 10. Криптографические методы защиты конфиденциальных документов

1. Программные и криптографические меры защиты электронных документов и конфиденциальных сведений
2. Представление о методах криптографии.
3. Сравнение методов и средств шифрования.
4. Программные средства криптографической защиты конфиденциальных данных.
5. Моделирование ситуации с установкой и настройкой сертифицированных программных средств криптографической защиты электронных документов и файлов, содержащих конфиденциальные, секретные данные.
6. Устный опрос.

Практическая часть:
Выполнение заданий по шифрованию/дешифрации электронных документов и архивов.

Практическое занятие 11, 12. Подготовка конфиденциальных дел и документов для архивного хранения. Подготовка конфиденциальных дел и документов для уничтожения

Теоретическая часть
Темы докладов:

1. Правовая база передачи документов на архивное хранение и уничтожение.
2. Экспертиза ценности конфиденциальных документов. Требования, предъявляемые к экспертизе. Задачи, функции, состав и порядок работы экспертной комиссии.
3. Этапы проведения экспертизы ценности документов. Особенности экспертизы ценности машиночитаемых, аудиовизуальных, конструкторских, технологических и научно-технических документов.
4. Требования к процессу уничтожения документов в соответствии со степенью их конфиденциальности. Порядок уничтожения печатных форм, брака и документирование результатов уничтожения в соответствии с уровнем грифа конфиденци-

альности. Назначение и задачи стадии уничтожения документов и носителей информации. Процедура отбора документов и носителей информации для уничтожения. Процедура уничтожения документов и носителей информации.

5. Порядок составления и оформления акта о выделении к уничтожению документов, не подлежащих хранению. Требования по включению в акт документов, дел и носителей информации.
6. Средства и способы уничтожения конфиденциальной информации. Программные и технические средства защиты цифровых (электронных) документов, носителей/хранилищ /каналов передачи данных.
7. Подготовка к уничтожению бумажных, машиночитаемых, аудиовизуальных, конструкторских, Способы и состав технологических операций уничтожения документов на различных носителях информации. Технические средства выполнения процедур уничтожения конфиденциальной информации и конфиденциальных документов.
8. Задачи и стадии подготовки и передачи дел в архив. Способы размещения в хранилище машиночитаемых, аудиовизуальных, технических, технологических и научно-технических документов. Оптимальные условия сохранности документов: противопожарная безопасность, температурно-влажностный, световой, санитарно-гигиенический и иные режимы.
9. Требования к охране и порядку доступа в архив. Правила работы сотрудников архива и посетителей. Порядок доступа к документам архива, при выдаче документов и дел. Сроки выдачи. Оформление возврата дел. Порядок выдачи документов и дел другим учреждениям, организациям и фирмам.
10. Порядок обращения с конфиденциальными документами. Режим хранения конфиденциальных документов. Проведение служебного расследования в случае возникновения ситуаций, отрицательно влияющих на качество информации.
11. Устный опрос.

Модуль 4

Практическое занятие 13. Технологии реализации защищенного электронного документооборота

Теоретическая часть

Темы докладов:

1. Электронная подпись и другие средства и методы защиты электронных документов при их автоматизированной обработке.
2. Виды электронной подписи, порядок ее использования
3. Порядок получения и использования защищенной цифровой (электронной) подписи.
4. Меры обеспечения безопасности информации в бумажном и электронном конфиденциальном документообороте.
5. Информационные системы и электронный документооборот (с конкретными примерами и областями использования)
6. Устный опрос.

Практическое занятие 14, 15, 16. Подготовка конфиденциальных дел и документов для архивного хранения. Подготовка конфиденциальных дел и документов для уничтожения.

Теоретическая часть

Темы докладов:

1. Экспертиза ценности конфиденциальных документов. Требования, предъявляемые к экспертизе.
2. Задачи, функции, состав и порядок работы экспертной комиссии. Этапы проведения экспертизы ценности документов.
3. Особенности экспертизы ценности машиночитаемых, аудиовизуальных, конструкторских, технологических и научно-технических документов.
4. Проверка наличия конфиденциальных документов.
5. Оформление результатов экспертизы. Порядок комплектования ведомственного архива и классификация хранилищ документов.
6. Учет конфиденциальных деловых (управленческих), технических, технологических и научно-технических документов в архиве.
7. Порядок реализации разрешительной системы при выдаче документов и дел.
8. Сроки выдачи. Оформление возврата дел. Порядок выдачи документов и дел другим учреждениям, организациям и фирмам.
9. Принципы размещения архивных дел в хранилище. Состав и типы используемого оборудования. Особенности размещения дел с особо важными конфиденциальными документами. Способы размещения в хранилище машиночитаемых, аудиовизуальных, технических, технологических и научно-технических документов. Оптимальные условия сохранности документов: противопожарная безопасность, температурно-влажностный, световой, санитарно-гигиенический и иные режимы.
10. Правовая база передачи на архивное хранение и уничтожение документов, в т.ч. содержащих конфиденциальные сведения и секретную информацию.
11. Процедура отбора документов и носителей информации для уничтожения.
12. Порядок составления и оформления акта с выделении к уничтожению документов, не подлежащих хранению. Требования по включению в акт документов, дел и носителей информации.
13. Подготовка к уничтожению бумажных, машиночитаемых, аудиовизуальных, конструкторских, технологических и научно-технических документов.
14. Процедура уничтожения документов и носителей информации. Порядок уничтожения печатных форм, брака и документирование результатов уничтожения в соответствии с уровнем грифа конфиденциальности.
15. Требования к процессу уничтожения документов в соответствии со степенью их конфиденциальности. Способы и состав технологических операций уничтожения документов на различных носителях информации.
16. Порядок внесения отметок об уничтожении документов и носителей информации в учетные формы.
17. Средства организационной техники, используемые при выполнении процедуры уничтожения конфиденциальной информации.

Практическая часть

1. Оформление документов на списание /уничтожение.
2. Процедура уничтожения конфиденциального документа.
3. Процедура подготовки дела или электронного носителя к передаче на архивное хранение.
4. Выполнение заданий по подготовке дел к списанию/уничтожению, оформление сопроводительных документов, в т.ч. электронных носителей .

Критерии оценки деятельности студента на практическом занятии:

0-5 балла - за 1 практическое задание - в зависимости от правильности и полноты решения задач практической части 8 занятий, где предполагается практическая часть (см. выше).

0-4 балла – за 1 доклад семинара, темы докладов приводятся в теоретической части практического занятия (количество баллов за доклад зависит от полноты изложения и актуальности информации). Студент может подготовить до 5 докладов в течение семестра.

Лабораторные занятия
Типовые задания

Лабораторное занятие 1. Движение, реквизиты конфиденциальных документов.

Практическая часть:
Оформление видов документов: организационных, распорядительных, справочно-информационных, научно-технических (практическое задание – оформить документы по образцу в офисном приложении). Реквизиты ограничения доступа конфиденциальных документов.
Устный опрос.

Лабораторная работа 2, 3. Технологии реализации защищенного электронного документооборота

Теоретическая часть
1. Основные угрозы электронным носителям информации и электронным документам
2. Риски цифровизации и автоматизации деловых процессов, связанные с заменой бумажного документооборота электронным и возрастанием информационных рисков.
3. Работа с конфиденциальными документами в сетях.
4. Риски облачных хранилищ при использовании программных средств электронного документооборота.
5. Меры безопасности при работе с почтовыми службами.
6. Меры технической защиты конфиденциальной информации.
7. Организационные меры защиты конфиденциальности электронных документов
8. Нормативно-правовая основа защиты конфиденциальных сведений.
9. Технологии реализации защищенного электронного документооборота
10. Электронная подпись

Лабораторное занятие 4,5. Учет конфиденциальных документов. Знакомство с возможностями защищенного электронного документооборота на примере конкретной СЭД (DirectumRX)

Практическая часть:
Практическое знакомство с системой электронного документооборота и средствами защиты конфиденциального документооборота этой СЭД (например, DirectumRX). Задание выполняется по пошаговой инструкции (*подробное описание действий и конкретные задания приводится в почтовой рассылке студентам, содержащим лекционный материал*).
Устный опрос.

Лабораторное занятие 6,7. Оперативное хранение конфиденциальных документов.

Практическая часть
1. Заполнение граф номенклатуры дел на конкретном примере. Задание на формирование и хранение дела, содержащего конфиденциальные документы.
2. Практическое задание по созданию, движению, поиску электронного документа в СЭД DirectumRX.

3. Устный опрос.
4. **Практическая часть** – деловая игра «Проверка наличия конфиденциальных документов или носителей конфиденциальных данных» (2 часа).

- Процедура проверки документов, дел и носителей информации
- Оформление результата проверки документов, дел и носителей информации. Ситуация моделируется в форме проверки «комиссией» -группой проверяющих по 3-4 студента, отчет предоставляется в виде электронного/бумажного отчета.

Лабораторное занятие 8. Технологии реализации защищенного электронного документооборота на примере конкретных программ

Практическая часть:

1. Знакомство с возможностями защищенного документооборота некоторых системы электронного документооборота (на примере СЭД DirectumRX, на примере средств защиты информации в пакете MS Office и др.)
2. Использование СЭД DirectumRX для разработки электронных документов по заданиям.
3. Другие ИС, СЭД для реализации работы с конфиденциальными документами.
4. Выполнение заданий по созданию электронных документов (типа ОРД) по пошаговой инструкции в СЭД.
5. Тестирование.

Критерии оценки деятельности студента на лабораторном занятии:

0-4 балла - за 1 занятие Модулей 1 и 3 - в зависимости от правильности и полноты решения задач практической части занятий, где предполагается практическая часть (см. выше), либо за доклад, если занятие проводится в виде семинара.

0-5 балла – за занятие Модулей 2 и 4, в зависимости от правильности и полноты решения задач практической части занятий, где предполагается практическая часть (см. выше), либо за доклад, если занятие проводится в виде семинара.

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.

1. Какие сведения относятся к конфиденциальным, согласно Указу Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера»
а) сведения, составляющие коммерческую тайну;
б) сведения о первых лицах государства;
в) сведения о золотовалютном фонде РФ;
г) сведения о законах, вступивших в силу.

2. Какой нормативный документ предусматривает установление для определенной информации ограничения на ее предоставление или распространение
а) ФЗ РФ « О персональных данных»;
б) ФЗ РФ «Об информации, информационных технологиях и о защите информацию»;
в) Уголовный Кодекс РФ;
г) Гражданский Кодекс РФ.

3.Что из нижеперечисленного не относится к конфиденциальной информации

а) государственная тайна
б) коммерческая тайна
в) персональные данные
г) общедоступная информация

4. Несанкционированный доступ определяется, как:
а) доступ субъектов к информации, нарушающий установленные правила разграничения доступа
б) доступ субъектов к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС
в) доступ к информации субъектов доступа не имеющих полномочий на доступ к СВТ АС
г) доступ к информации с использованием технических средств съема информации (закладные устройства, портативные и средства ведения информационной разведки)

5. Обладатель информации вправе. Отметьте правильные варианты ответов:
а) разрешать или ограничивать доступ к информации; определять порядок и условия такого доступа распространять ее по своему усмотрению
б) передавать информацию другим лицам по договору или на ином установленном законом основании
в) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами
г) защищать любыми доступными способами и средствами свои права в случае незаконного получения информации или ее незаконного использования иными лицами

Критерии оценки тестирования: Тест из 25 правильно выполненных заданий оценивается в 20 баллов.

Типовые задания для контрольной самостоятельной работы

Цель проведения контрольной работы – оценка уровня владения знаниями в области защищенного документооборота. Контрольная работа проводится в письменной форме, защищается студентами на предпоследнем практическом занятии (путем краткого выступления или ответа на вопросы, связанные с содержанием контрольной работы и спец.терминами).

Темы самостоятельной контрольной работы

1. Роль конфиденциальных документа в жизни человека и общества.
2. Документы в сфере защиты информации.
3. Влияние технических достижений на защиту конфиденциальных документов.
4. Документ как способ фиксации конфиденциальной и секретной информации.
5. Понятие оперативной и ретроспективной (исторической) конфиденциальной документной информации.
6. Понятие ценности документной информации, факторы, влияющие на информационную ценность документа.
7. Влияние материала носителя на долговечность документа и сохранность информации.
8. Нормативная регламентация защиты документированной информации.
9. Государственные стандарты по защите информации.
10. Требования к составлению и оформлению конфиденциальных документов.
11. Теоретические основы экспертизы ценности конфиденциальных документов.
12. Деятельность Межведомственной комиссии по защите государственной тайны.

13. Государственное регулирование вопросов, связанных с защитой и обработкой конфиденциальных документов.
14. Потоки конфиденциальных документов. Понятие «Защищенный документооборот».
15. Порядок разработки перечня конфиденциальных документов.
16. Локальные нормативно-методические документы по конфиденциальному делопроизводству.
17. Состав технологических этапов и операций конфиденциальных документов.
18. Прием, предварительное рассмотрение поступивших конфиденциальных документов.
19. Технология отправки конфиденциальных документов.
20. Особенности оформления издаваемых конфиденциальных документов.
21. Система доступа к конфиденциальным документам.
22. Структура защищаемых документопотоков.
23. Учет конфиденциальных документов.
24. Порядок рассмотрения и исполнения конфиденциальных документов.
25. Размножение конфиденциальных документов.
26. Контроль исполнения конфиденциальных документов.
27. Составление и оформление номенклатуры дел.
28. Формирование и хранение дел, содержащих конфиденциальные документы.
29. Уничтожение конфиденциальных документов.
30. Проверка наличия конфиденциальных документов.
31. Порядок комплектования ведомственного архива конфиденциальной документации и классификация хранилищ документов.
32. Учет деловых (управленческих) и научно-технических документов в архиве.
33. Обеспечение сохранности конфиденциальных документов.
34. Научно-справочный аппарат к архивам конфиденциальных документов.
35. Порядок использования конфиденциальных архивных документов.
36. Оборудование архивохранилищ.
37. Виртуальные защищенные сети VPN.
38. Безопасность межсетевого обмена данными.
39. Эволюция систем обработки и хранения документов.
40. Технологии электронного документооборота.
41. Компоненты систем электронного документооборота.
42. Жизненный цикл документа в системах электронного документооборота.
43. Типовые требования к системам электронного документооборота.
44. Интерфейс, архитектура и требования безопасности систем электронного документооборота.
45. Место системы электронного документооборота в информационной системе предприятия.
46. Модульность системы электронного архива.
47. Автоматизированное рабочее место.
48. Деловая почта. Методы борьбы со спамом.
49. Совершенствование носителей документированной информации.
50. Организационные и методические проблемы автоматизации делопроизводственных операций.
51. Локальная автоматизация операций учета документов.
52. Функциональные возможности систем комплексной автоматизации.
53. Конфиденциальные документы вычислительного центра.
54. Электронная подпись документов как методика обеспечения защищенного документооборота.
55. Защита электронных документов.
56. Уничтожение электронных документов.
57. Представление документов в электронном виде. Электронные издания.

58. Объекты защиты в компьютерных информационных системах.

Критерии и методика оценивания самостоятельной работы. Самостоятельная работа выполняется в форме исследования, выполненного по 5 **вопросам** из вышеприведенного списка. Каждый из 5 пунктов (тем) раскрывается отдельно и оценивается по следующим критериям:

- 3 балла выставляется студенту за 1 тему (из 2), если тема полностью раскрыта, в тексте отчета отсутствует плагиат (чужой текст без ссылок на источники). Доля собственного текст студента (не заимствованного в сети) должна составлять не менее 40%. Любые цитаты должны иметь ссылки на источник. Источники не должны быть устаревшими (более 4-летней давности).

- 2 балла, если доля собственного текста по 1 теме студента не превышает 1/3 от всего отчета (процент оригинальности проверяется системой Антиплагиат) и/или если первоисточники, которые цитирует или иначе использует студент, устарели (на 5-10 лет).

- 1 балл, если отчет по теме содержит плагиат, доля заимствований велика и/или источники сведений устарели на 10 и более лет.

Результат по каждой из трех тем отчета самостоятельной контрольной работы суммируется. Общая сумма за самостоятельную контрольную работу не превышает 20 баллов. Баллы за КСР выставляются студенту после защиты контрольной работы на предпоследнем практическом занятии.

Типовые вопросы зачетного собеседования в 6 семестре:

1. Правовые акты и законы, регулирующие защиту конфиденциальной информации (и дать краткую характеристику содержанию законов, регулирующих обращение с конфиденциальной информацией).
2. Виды конфиденциальной информации.
3. Угрозы конфиденциальной информации.
4. Обзор организационных и технических мер обеспечения безопасности информации, содержащейся в электронных и бумажных конфиденциальных документах.
5. Организация конфиденциального делопроизводства.
6. Функции подразделения конфиденциального делопроизводства.
7. Перечни конфиденциальных сведений.
8. Понятие конфиденциального делопроизводства. Перечни конфиденциальных документов.
9. Система доступа к конфиденциальным документам.
10. Учет носителей конфиденциальной информации. Учет издаваемых конфиденциальных документов.
11. Получение конфиденциальных документов и их учет.
12. Отправление конфиденциальных документов.
13. Порядок копирования конфиденциальных документов.
14. Организация исполнения конфиденциальных документов.
15. Номенклатура конфиденциальных дел. Формирование конфиденциальных дел. Оформление конфиденциальных дел.
16. Подготовка конфиденциальных дел и документов для архивного хранения.
17. Требования к помещениям подразделения конфиденциального делопроизводства. Передача помещений конфиденциального делопроизводства под охрану.
18. Порядок обращения с конфиденциальными документами.
19. Контроль наличия конфиденциальных документов.
20. Подготовка к проведению конфиденциальных совещаний. Порядок проведения конфиденциальных совещаний.
21. Проведение внутренних расследований по фактам утраты конфиденциальных доку-

ментов или разглашения конфиденциальной информации.

22. Особенности защиты информации в системах электронного документооборота. Понятие и формы реализации защищенного электронного документооборота.

Критерии оценки результатов собеседования (в баллах):

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

Зачет в 6 семестре

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

- «Зачтено» выставляется студенту, если он набрал по результатам изучения дисциплины 60 баллов;

- «Не зачтено» выставляется студенту, если он набрал менее 59 баллов.

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

5. Учебно-методическое и информационное обеспечение дисциплины

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

а) основная учебная литература:

1. Автоматизация документооборота [Электронный ресурс] : учебное пособие / А.А. Тищенко [и др.]. — Электрон. дан. — Москва : ФЛИНТА, 2018. — 108 с. — Режим доступа: https://e.lanbook.com/book/113481
2. Доброва, О.В. Документирование управленческой деятельности [Электронный ресурс] : учебно-методическое пособие / О.В. Доброва. — Электрон. дан. — Пенза : ПензГТУ, 2014. — 52 с. — Режим доступа: https://e.lanbook.com/book/62484.
3. Костыгова, Л.А. Документирование управленческой деятельности. Курс лекций [Электронный ресурс] : учебное пособие / Л.А. Костыгова. — Электрон. дан. — Москва : МИСИС, 2012. — 85 с. — Режим доступа: https://e.lanbook.com/book/64450.

б) дополнительная учебная литература:

4. Куняев Н.Н., Уралов Д.Н. Документоведение: учебник / Н.Н. Куняев, Д.Н. Уралов. – Логос, 2014 – 244 с. – Режим доступа http://biblioclub.ru/book/231590/
5. Максимов Н.В., Голицына О.Л., Тихомиров Г.В., Храмцов П.Б.Информационные ресурсы и поисковые системы: учебное пособие. - М.: МИФИ, 2008. – 400 с. http://biblioclub.ru/index.php?page=book&id=231125&sr=1

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

1. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru.
2. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
3. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
4. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
5. www.fstec.ru –сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
1. *учебная аудитория для проведения занятий лекционного типа:* аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гу-	Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1

манитарный корпус), аудитория № 516 (гуманитарный корпус). **2.** ***учебная аудитория для проведения лабораторных работ:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **3.** ***учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **4.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (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.** ***учебная аудитория для текущего контро-***		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. **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. **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт. 1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition.

ля и промежуточной аттестации: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **6.*помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **7.*помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 523 (гуманитарный корпус).		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.

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 и обработка конфиденциальных документов**»
на 6 семестр ОФО

Вид работы	Объем дисциплины
	ОФО
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	48,2
лекций	16
практических/ семинарских	16
лабораторных	16
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	59,8
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	

Содержание рабочей программы
дисциплины «**Защита и обработка конфиденциальных документов**»
на 7 семестр ОФО

Вид работы	Объем дисциплины
	ОФО
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	37,2
лекций	18
практических/ семинарских	18
лабораторных	
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	72
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	34,8

Форма контроля
Зачет 6 семестр
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	СРС			
1	2	4	5	6	7	8	9	10
	Модуль 1 (6 семестр)							
1	**Тема 1.** Основные понятия курса, Конфиденциальная информация **Содержание:** Цели защиты конфиденциальной информации. Основные термины и определения. Виды тайн и их классификация. Основные способы защиты конфиденциальной информации. Основные задачи конфиденциального делопроизводства. Перечень конфиденциальных сведений. Разработка перечня конфиденциальных сведений. Форма перечня конфиденциальных сведений. Грифы и сроки конфиденциальности документов. Степень конфиденциальности. Система доступа к конфиденциальным документам. Правовые основы защищенного документооборота.	2	2	2	4,8	1-5	Самостоятельное изучение рекомендуемых источников и материалов, выполнение практических заданий, подготовка к семинару, тестирование, контрольная СР.	КР, ПЗ, ЛЗ, опрос, Т, З
2	**Тема 2.** Нормативная база, регулирующая обработку конфиденциальной и секретной информации	4	4	4	15	1-5	Самостоятельное изучение рекомендуемых источников и материалов, выполнение практических заданий, подготовка к семинару,	КР, ПЗ, ЛЗ, опрос, Т, З

							тестирование, контрольная СР.	
	Модуль 2							
2	**Тема 3.** Движение конфиденциальных документов. **Содержание:** Системы документации. Подготовка и издание конфиденциальных документов. Реквизиты ограничения доступа к документу. Оформление некоторых видов документов: организационных, распорядительных, справочно-информационных, научно-технических, научно-исследовательских. Учет носителей конфиденциальной информации. Учет поступивших конфиденциальных документов. Отправление конфиденциальных документов.	4	4	4	15	1-5	Самостоятельное изучение рекомендуемых источников и материалов, выполнение практических заданий, подготовка к семинару, тестирование, контрольная СР.	КР, ПЗ, ЛЗ, опрос, Т, З
3	**Тема 4.**Учет конфиденциальных документов. **Содержание:** Структура защищенного документооборота. Документопотоки: входящий.издаваемый, выделенного хранения. Состав технологических этапов и операций. Сущность задачи и особенности конфиденциального делопроизводства. Принципы распределения документов между руководителями, структурными подразделениями и специалистами. Функциональная принадлежность документированной информации. Уровень компетенции должностных лиц решении вопросов, поставленных в документах. Реализация порядка доступа к конфиденциальным документам. Общие требования к учету конфиденциальных документов. Учет изданных, поступивших конфиденциальных документов. Учет конфиденциальных документов выделенного хранения. Журналы или картотеки учета изданных и поступивших документов, в т.ч. конфиденциальных распорядительных документов, протоколов, входящих конфиденциальных пакетов. Журналы учета, подлежащих выделенному хранению. Копирование и размножение конфиденциальных документов. Разрешение на размножение документов. Журнал учета размножения конфиденциальных документов.	4	4	4	15	1-5	Самостоятельное изучение рекомендуемых источников и материалов, выполнение практических заданий, подготовка к семинару, тестирование, контрольная СР.	КР, ПЗ, ЛЗ, опрос, Т, З
4	**Тема 4.** Оперативное хранение конфиденциальных документов. **Содержание:** Составление и оформление номенклатуры дел. Разработка номенклатуры дел. Формирование конфиденци-	2	2	2	10	1-5	Самостоятельное изучение рекомендуемых источников и материалов, вы-	КР, ПЗ, ЛЗ, опрос, Т, З

	альных дел. Номенклатура конфиденциальных дел. Гриф конфиденциальности номенклатур дел. Составление заголовков дел. Заполнение граф номенклатуры дел. Справка-заместитель. Опись документов дела. Карточка учета выдачи дела. Заверительная надпись дела. Дополнительные требования к формированию в дела конфиденциальных документов. Нумерация листов. Заполнение описи документов дела. Составление заверительной надписи. Прошивка и опечатывание дела. Оформление карточки учета выдачи дела Формирование и хранение дел, содержащих конфиденциальные документы.						полнение практических заданий, подготовка к семинару, тестирование, контрольная СР.	
	Всего в 6 семестре	16	16	16	59,8			

	Модуль 3 (7 семестр)							
5	**Тема 5.** Учет, движение, проверка наличия конфиденциальных документов. Криптозащита (шифрование) как мера защиты КИ. **Содержание.** Назначение и задачи проверки наличия документов, дел и носителей информации. Сферы распространения проверки. Требования, предъявляемые к проверке. Виды проверок. Периодичность проверок наличия и уровень конфиденциальности информации. Проверки регламентированные (периодические) и нерегламентированные (непериодические). Типовой состав процедур и операций проверки наличия. Оформление результата проверки. Состав проверяемых документов. Проверка наличия документов, дел и носителей информации при увольнении сотрудника. Ее цели и оформление результата проверки. Порядок приема от увольняющегося сотрудника документов, дел и носителей информации. Проверка наличия и сохранности баз данных в ЭВМ. Цели проверки и порядок ее проведения. Оформление результата проверки. Криптозащита (шифрование) как мера зашиты КИ. Программно-технические средства шифрования, нормативно-правовое регулирование сферы криптозащиты.	6	4		20	1-5	Самостоятельное изучение рекомендуемых источников и материалов, выполнение практических заданий, подготовка к семинару, тестирование, контрольная СР.	КР, ПЗ, ЛЗ, опрос, Т, З
6	**Тема 6.** Подготовка конфиденциальных дел и документов для архивного хранения. Подготовка конфиденциальных дел и документов для уничтожения.	5	6		18	1-5	Самостоятельное изучение рекомендуемых источников	КР, ПЗ, ЛЗ, опрос, Т, З

	Содержание. Назначение и задачи стадии подготовки и передачи дел в архив. Экспертиза ценности конфиденциальных документов. Требования, предъявляемые к экспертизе. Задачи, функции, состав и порядок работы экспертной комиссии. Этапы проведения экспертизы ценности документов. Проверка наличия конфиденциальных документов. Оформление результатов экспертизы. Особенности экспертизы ценности машиночитаемых, аудиовизуальных, конструкторских, технологических и научно-технических документов. Порядок комплектования ведомственного архива и классификация хранилищ документов. Учет конфиденциальных деловых (управленческих), технических, технологических и научно-технических документов в архиве. Научно-справочный аппарат к архивам документов, порядка использования конфиденциальных архивных документов; оборудованию архивохранилищ. Порядок реализации разрешительной системы при выдаче документов и дел. Сроки выдачи. Оформление возврата дел. Порядок выдачи документов и дел другим учреждениям, организациям и фирмам. Принципы размещения архивных дел в хранилище. Состав и типы используемого оборудования. Особенности размещения дел с особо важными конфиденциальными документами. Способы размещения в хранилище машиночитаемых, аудиовизуальных, технических, технологических и научно-технических документов. Оптимальные условия сохранности документов: противопожарная безопасность, температурно-влажностный, световой, санитарно-гигиенический и иные режимы. Требования к охране и порядку доступа в архив. Правила работы сотрудников архива и посетителей. План эвакуации архива в экстремальных ситуациях. Страховые фонды документов, их учет. Режим хранения конфиденциальных документов. Порядок обращения с конфиденциальными документами. Проведение служебного Расследования в случае возникновения ситуаций, отрицательно влияющих на качество информации.						и материалов, выполнение практических заданий, подготовка к семинару, тестирование, контрольная СР.	
	Модуль 4							
7	**Тема 7**. Технологии реализации защищенного электронного документооборота.	4	4		18	1-5	Самостоятельное изучение рекомен-	КР, ПЗ, ЛЗ, опрос, Т, З

	Содержание. Конкретные способы и технологии реализации защищенного электронного документооборота в ИС, СЭД (с примерами). Электронная подпись и другие средства и методы защиты электронных документов при их автоматизированной обработке. Криптографические меры защиты электронных документов, информации.						дуемых источников и материалов, выполнение практических заданий, подготовка к семинару, тестирование, контрольная СР.	
8	**Тема 8.** Уничтожение конфиденциальных документов. **Содержание.** Порядок уничтожения печатных форм, брака и документирование результатов уничтожения в соответствии с уровнем грифа конфиденциальности. Процедура отбора документов и носителей информации для уничтожения. Порядок составления и оформления акта с выделении к уничтожению документов, не подлежащих хранению. Требования по включению в акт документов, дел и носителей информации. Подготовка к уничтожению бумажных, машиночитаемых, аудиовизуальных, конструкторских, технологических и научно-технических документов. Правовая база передачи на архивное хранение и уничтожение. Процедура уничтожения документов и носителей информации. Требования к процессу уничтожения документов в соответствии со степенью их конфиденциальности. Способы и состав технологических операций уничтожения документов на различных носителях информации. Порядок внесения отметок об уничтожении документов и носителей информации в учетные формы. Средства организационной техники, используемые при выполнении процедуры уничтожения конфиденциальной информации.	4	4		20	1-5	Самостоятельное изучение рекомендуемых источников и материалов, выполнение практических заданий, подготовка к семинару, тестирование, контрольная СР.	КР, ПЗ, ЛЗ, опрос, Т, З
	Всего	18	18		72			

ПЗ –практическое задание (или семинар), Т – тестирование, КР – выполнение контрольной самостоятельной работы (темы см. выше), З – зачетное собеседование.

Приложение 2
Рейтинг – план дисциплины
Защита и обработка конфиденциальных документов

Направление подготовки **10.03.01 Информационная безопасность**
Курс 3, семестр 6

Виды учебной деятельности студентов	**Балл за конкретное задание**	**Число заданий за семестр**	**Баллы**	
			Минимальный	**Максимальный**
Модуль 1				
Текущий контроль				**20**
1.Аудиторная работа				
Доклады и здания	4	5	0	20
Рубежный контроль				**15**
Устный опрос	3	5	0	15
Всего				**35**
Модуль 2				
Текущий контроль				**30**
1.Аудиторная работа				
- Доклады и здания	5	6	0	30
Рубежный контроль				**35**
Тест	0,8	25	0	20
Зачет (собеседование)	15	1	0	15
Всего				**65**
Поощрительные баллы				
1.Публикация научной статьи	5	1	0	5
2.Участие в научно-практической конференции по профилю	5	1	0	5
Всего				**10**
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение лабораторных занятий	-	-	0	-10
ВСЕГО:			0	110

Рейтинг – план дисциплины
Защита и обработка конфиденциальных документов

Направление подготовки **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 3				
Текущий контроль				**20**
1.Аудиторная работа				
Доклады и здания	4	5	0	20
Рубежный контроль				**15**
Устный опрос	3	5	0	15
Всего				**35**
Модуль 4				
Текущий контроль				**20**
1.Аудиторная работа				
- Доклады и здания	5	6	0	30
Рубежный контроль				**15**
Отчет по контрольной самостоятельной работе	15	1	0	15
Всего				**45**
Поощрительные баллы				
1.Публикация научной статьи	5	1	0	5
2.Участие в научно-практической конференции по профилю	5	1	0	5
Всего				**10**
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
3. Посещение лекционных занятий			0	-6
4. Посещение лабораторных занятий	-	-	0	-10
Итоговый контроль				
Экзамен			**0**	**30**
ВСЕГО:			**0**	**110**