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

Актуализировано:
на заседании кафедры
протокол № 10 от «7» июня 2018 г.
Зав. кафедрой / А.С. Исмагилова

Согласовано:
Председатель УМК института
/ Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность автоматизированных систем

Б1.Б.32 (базовая)

программа бакалавриата

Направление
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации

Квалификация
бакалавр

Разработчик (составитель) / И.В. Салов

Для приема: 2015 г.

Уфа 2018

Составитель: И.В. Салов

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

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры государственного управления, протокол № __ от «__» _____ 201_ г.

Заведующий кафедрой _____/ _____Ф.И.О/

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

Заведующий кафедрой _____/ _____Ф.И.О/

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

Заведующий кафедрой _____/ _____Ф.И.О/

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

Заведующий кафедрой _____/ _____Ф.И.О/

Список документов и материалов

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

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	Знать основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ, основные понятия, цели, принципы, сферы применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, роль договоров в сфере информационной безопасности; виды юридической ответственности, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	– Способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)	
	Знать средства контроля контента, средства анализа защищенности и средства обнаружения атак для обеспечения безопасности в IP-сетях, средства защиты от несанкционированного доступа, применение межсетевых экранов	– Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)	
	Знать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты	– Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)	

	информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства		
	Знать нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом, стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем	– Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)	
	Знать технологии обеспечения защиты и сохранности конфиденциальных документов, системы организации бумажного и электронного конфиденциального делопроизводства, методы и средства защиты информации в операционных системах, базах данных и прикладных программах, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации	- Способность участвовать в разработке подсистемы управления информационной безопасностью (ПСК-1)	
Умения	Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу	– Способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)	

	профессиональной деятельности, и использовать их в своей деятельности, предвидеть юридические опасности и угрозы, связанные с использованием информации, и соблюдать основные правовые требования информационной безопасности, в т.ч. защиты интеллектуальной собственности; предпринимать необходимые меры по восстановлению нарушенных прав		
	Уметь использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность, использовать системы электронного документооборота, работать с информацией в глобальных компьютерных сетях	– Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)	
	Уметь выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации, применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе, разрабатывать организационно-распорядительные документы по вопросам	– Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)	

	защиты информации		
	Уметь интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	– Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)	
	Уметь конфигурировать и использовать средства защиты информации в СУБД, ОС и прикладных программах, настраивать антивирусные программы и другие средства борьбы с программными закладками, применять технические средства защиты данных	- Способность участвовать в разработке подсистемы управления информационной безопасностью (ПСК-1)	
Владения (навыки / опыт деятельности)	Владеть навыками анализа юридических последствий, связанных с использованием информации, опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	– Способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)	
	Владеть методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам, навыками	– Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей	

	работы с компьютером как средством защиты информации	функционирования объекта защиты (ОПК-7)	
	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации, методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	– Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)	
	Владеть интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач	– Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)	
	Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий	- Способность участвовать в разработке подсистемы управления информационной безопасностью (ПСК-1)	

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

Дисциплина «Информационная безопасность автоматизированных систем» относится к базовой части образовательной программы.

Дисциплина изучается на 4 курсе в 7-м семестре.

Цели изучения дисциплины: подготовка студентов к практическому использованию профессиональных средств информационных технологий в профессиональной деятельности.

Изучение дисциплины базируется на знаниях, умениях и навыках, сформированных в результате освоения студентами предшествующих дисциплин образовательной программы по направлению 10.03.01 Информационная безопасность профиля подготовки «Информационная безопасность автоматизированных систем»: «Документоведение», «Организационное и правовое обеспечение информационной безопасности», «Комплексная

система защиты информации на предприятии».

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

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

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

ОПК-5: Способность использовать нормативные правовые акты в профессиональной деятельности.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ	Не знает	Знает некоторые элементы основ российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ
	Знать основные понятия, цели, принципы, сферы применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, роль договоров в сфере информационной безопасности; виды юридической ответственности	Не знает	Знает некоторые основные понятия, цели, принципы, сферы применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, роль договоров в сфере информационной безопасности; виды юридической ответственности
	Знать методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	Не знает	Знает основные методы и средства правовой защиты интересов субъектов в сфере информационной безопасности
Второй этап (уровень)	Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности	Не умеет	Допускает незначительные ошибки при ориентировании в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности
	Уметь предвидеть юридические опасности и угрозы, связанные с использованием информации, и соблюдать основные правовые требования информационной безопасности, в т.ч. защиты интеллектуальной собственности; предпринимать необходимые меры по восстановлению нарушенных прав	Не умеет	Допускает незначительные ошибки при использовании навыков предвидения юридических опасностей и угроз, связанных с использованием информации, и соблюдать основные правовые требования информационной безопасности, в т.ч. защиты интеллектуальной собственности; предпринимать необходимые меры по восстановлению нарушенных прав
Третий этап (уровень)	Владеть навыками анализа юридических последствий, связанных с использованием информации	Не владеет	Владеет отдельными навыками анализа юридических последствий, связанных с использованием информации
	Владеть опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	Не владеет	Владеет отдельными элементами опыта работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности

ОПК-7: Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать средства контроля контента	Не знает	Знает основы средств контроля контента
	Знать средства анализа защищенности и средства обнаружения атак для обеспечения безопасности в IP-сетях	Не знает	Знает основные средства анализа защищенности и средства обнаружения атак для обеспечения безопасности в IP-сетях
	Знать средства защиты от несанкционированного доступа	Не знает	Знает основные средства защиты от несанкционированного доступа
	Знать применение межсетевых экранов	Не знает	Знает основу применения межсетевых экранов
Второй этап (уровень)	Уметь использовать базовые возможности информационных систем для решения задач фирмы	Не умеет	Допускает незначительные ошибки при использовании возможностей информационных систем для решения задач фирмы
	Уметь внедрять компоненты систем предприятия, обеспечивающие информационную безопасность	Не умеет	Допускает незначительные ошибки при внедрении компонентов систем предприятия, обеспечивающие информационную безопасность
	Уметь использовать системы электронного документооборота	Не умеет	Допускает незначительные ошибки при использовании системы электронного документооборота
	Уметь работать с информацией в глобальных компьютерных сетях	Не умеет	Допускает незначительные ошибки при работе с информацией в глобальных компьютерных сетях
Третий этап (уровень)	Владеть методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам	Не владеет	Владеет отдельными методиками определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам
	Владеть навыками работы с компьютером как средством защиты информации	Не владеет	Владеет отдельными навыками работы с компьютером как средством защиты информации

ПК-5: Способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации.

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 основные правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации
	Знать правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства	Не знает	Знает основные правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства
Второй этап (уровень)	Уметь выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации	Не умеет	Допускает незначительные ошибки при выборе типа необходимых средств для выявления наличия электронных средств перехвата информации
	Уметь применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе	Не умеет	Допускает незначительные ошибки при применении на практике методов локальной и комплексной автоматизации процессов обработки документов в документационной службе
	Уметь разрабатывать организационно-распорядительные документы по вопросам защиты информации	Не умеет	Допускает незначительные ошибки при разработке организационно-распорядительных документов по вопросам защиты информации
Третий этап (уровень)	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Не владеет	Владеет отдельными навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации
	Владеть методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	Не владеет	Владеет отдельными методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности

ПК-7: Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом	Не знает	Знает основные нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом
	Знать стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов	Не знает	Знает основные стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов
	Знать методики анализа рисков информационных систем	Не знает	Знает основные методики анализа рисков информационных систем
Второй этап (уровень)	Уметь интерпретировать и обобщать данные, формулировать выводы и рекомендации	Не умеет	Допускает незначительные ошибки при интерпретации и обобщении данных, формулировании выводов и рекомендаций
	Уметь применять на практике методы обработки данных	Не умеет	Допускает незначительные ошибки при применении на практике методов обработки данных
	Уметь разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	Не умеет	Допускает незначительные ошибки при разработке и реализации решений, направленных на поддержку социально-значимых проектов и развитие компьютерного творчества
Третий этап (уровень)	Владеть методами интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений	Не владеет	Владеет отдельными методами интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений
	Владеть методологией и навыками решения научных и практических задач	Не владеет	Владеет отдельными элементами методологии и навыкоы решения научных и практических задач

ПСК-1: Способность участвовать в разработке подсистемы управления информационной безопасностью.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
Первый этап (уровень)	Знать технологии обеспечения защиты и сохранности конфиденциальных документов, системы организации бумажного и электронного конфиденциального делопроизводства	Не знает	Знает основные технологии обеспечения защиты и сохранности конфиденциальных документов, системы организации бумажного и электронного конфиденциального делопроизводства
	Знать методы и средства защиты информации в операционных системах, базах данных и прикладных программах	Не знает	Знает основные методы и средства защиты информации в операционных системах, базах данных и прикладных программах
	Знать программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации	Не знает	Знает основные программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации
Второй этап (уровень)	Уметь конфигурировать и использовать средства защиты информации в СУБД, ОС и прикладных программах	Не умеет	Допускает незначительные ошибки при конфигурации и использования средств защиты информации в СУБД, ОС и прикладных программах
	Уметь настраивать антивирусные программы и другие средства борьбы с программными закладками, применять технические средства защиты данных	Не умеет	Допускает незначительные ошибки при настройке антивирусных программ и других средств борьбы с программными закладками, применении технических средств защиты данных
Третий этап (уровень)	Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий	Не владеет	Владеет отдельными навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий

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	Знать основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ, основные понятия, цели, принципы, сферы применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов, роль договоров в сфере информационной безопасности; виды юридической ответственности, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности	ОПК-5	тестирование, практическое задание, контрольная работа, лабораторная работа
	Знать средства контроля контента, средства анализа защищенности и средства обнаружения атак для обеспечения безопасности в IP-сетях, средства защиты от несанкционированного доступа, применение межсетевых экранов	ОПК-7	тестирование, практическое задание, контрольная работа, лабораторная работа
	Знать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного	ПК-5	тестирование, практическое задание, контрольная работа, лабораторная работа

	конфиденциального делопроизводства		
	Знать нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом, стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем	ПК-7	тестирование, практическое задание, контрольная работа, лабораторная работа
	Знать технологии обеспечения защиты и сохранности конфиденциальных документов, системы организации бумажного и электронного конфиденциального делопроизводства, методы и средства защиты информации в операционных системах, базах данных и прикладных программах, программные средства борьбы со злонамеренным программным обеспечением; аппаратные средства борьбы с утечкой информации	ПСК-1	тестирование, практическое задание, контрольная работа, лабораторная работа
2-й этап Уметь	Уметь ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности, предвидеть юридические опасности и угрозы, связанные с использованием информации, и соблюдать основные правовые требования информационной безопасности, в т.ч. защиты	ОПК-5	тестирование, практическое задание, контрольная работа, лабораторная работа

	интеллектуальной собственности; предпринимать необходимые меры по восстановлению нарушенных прав		
	Уметь использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность, использовать системы электронного документооборота, работать с информацией в глобальных компьютерных сетях	ОПК-7	тестирование, практическое задание, контрольная работа, лабораторная работа
	Уметь выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации, применять на практике методы локальной и комплексной автоматизации процессов обработки документов в документационной службе, разрабатывать организационно-распорядительные документы по вопросам защиты информации	ПК-5	тестирование, практическое задание, контрольная работа, лабораторная работа
	Уметь интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	ПК-7	тестирование, практическое задание, контрольная работа, лабораторная работа

	Уметь конфигурировать и использовать средства защиты информации в СУБД, ОС и прикладных программах, настраивать антивирусные программы и другие средства борьбы с программными закладками, применять технические средства защиты данных	ПСК-1	тестирование, практическое задание, контрольная работа, лабораторная работа
3-й этап Владеть	Владеть навыками анализа юридических последствий, связанных с использованием информации, опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности	ОПК-5	тестирование, практическое задание, контрольная работа, лабораторная работа
	Владеть методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам, навыками работы с компьютером как средством защиты информации	ОПК-7	тестирование, практическое задание, контрольная работа, лабораторная работа
	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации, методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	ПК-5	тестирование, практическое задание, контрольная работа, лабораторная работа

	Владеть интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач	ПК-7	тестирование, практическое задание, контрольная работа, лабораторная работа
	Владеть навыками эксплуатации современного электронного оборудования и информационно-коммуникационных технологий	ПСК-1	тестирование, практическое задание, контрольная работа, лабораторная работа

4.3. Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 1.

Типовые вопросы для зачета

1. Понятие, виды и структура АИС.
2. Общая характеристика составляющих, методов и механизмов обеспечения информационной безопасности АИС
3. Дискреционные и мандатные модели разграничения доступа к информации в АИС
4. Модели ролевого доступа и технологии рабочих групп пользователей
5. Тематическое разграничение доступа к информации в документальных АИС)
6. Место и роль автоматизированных систем в управлении бизнес-процессами.
7. Защита автоматизированных систем как процесс управления рисками.
8. Методы оценки целесообразности затрат на обеспечение безопасности.
9. Особенности современных автоматизированных систем как объектов защиты.
10. Определение безопасности автоматизированных систем.
11. Информация и информационные ресурсы.
12. Субъекты информационных отношений, их безопасность.
13. Цель защиты автоматизированной системы и циркулирующей в ней информации.
14. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем.
15. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений.
16. Классификация угроз безопасности.
17. Классификация каналов проникновения в автоматизированную систему и утечки информации.
18. Неформальная модель нарушителя.
19. Виды мер противодействия угрозам безопасности.
20. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.
21. Защищаемая информация.
22. Лицензирование.
23. Сертификация средств защиты информации и аттестация объектов информатизации.
24. Специальные требования и рекомендации по технической защите

конфиденциальной информации.
25. Юридическая значимость электронных документов с электронной подписью.
26. Ответственность за нарушения в сфере защиты информации.
27. Государственная система защиты информации.
28. Контроль состояния защиты информации.
29. Технология управления безопасностью информации и ресурсов в автоматизированной системе.
30. Институт ответственных за обеспечение информационной безопасности.
31. Регламентация действий пользователей и обслуживающего персонала автоматизированной системы.
32. Политика безопасности организации.
33. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты.
34. Распределение функций по обеспечению безопасности автоматизированных систем.
35. Организационно-распорядительные документы по обеспечению безопасности автоматизированных систем.
36. Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях.
37. Регламентация правил парольной и антивирусной защиты.
38. Регламентация порядка допуска к работе и изменения полномочий пользователей автоматизированной системы.
39. Регламентация порядка изменения конфигурации аппаратно-программных средств автоматизированной системы.
40. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач.
41. Категорирование и документирование защищаемых ресурсов.
42. Концепция информационной безопасности организации.
43. План защиты информации.
44. План обеспечения непрерывной работы и восстановления подсистем автоматизированной системы.
45. Основные механизмы защиты автоматизированных систем.
46. Защита периметра компьютерных сетей и управление механизмами защиты.
47. Страхование информационных рисков.
48. Аппаратно-программные средства защиты информации от несанкционированного доступа.
49. Средства аппаратной поддержки.
50. Способы аутентификации.
51. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа.
52. Защита от вмешательства в процесс нормального функционирования автоматизированной системы.
53. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы.
54. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.
55. Типовая корпоративная сеть.
56. Уровни информационной инфраструктуры корпоративной сети.
57. Уязвимости и их классификация.
58. Классификация атак.
59. Средства защиты сетей.
60. Угрозы, связанные с периметром корпоративной сети.

61. Составляющие защиты периметра.
62. Межсетевые экраны.
63. Анализ содержимого почтового и веб-трафика.
64. Виртуальные частные сети.
65. Управление уязвимостями.
66. Архитектура систем управления уязвимостями.
67. Особенности сетевых агентов сканирования.
68. Средства анализа защищенности системного уровня.
69. Управление журналами событий.
70. Категории журналов событий.
71. Инфраструктура управления журналами событий.
72. Введение в технологию обнаружения атак.
73. Классификация систем обнаружения атак.

Критерии оценивания

Критериями оценивания для студентов очной формы обучения 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).

Темы лабораторных работ

Цель проведения лабораторных работ – практическое освоение материала дисциплины.

1) Принципы построения системы обеспечения безопасности информации в автоматизированной системе.
2) Правовые основы обеспечения безопасности автоматизированных систем.
3) Организационно-распорядительные документы по обеспечению безопасности автоматизированных систем.
4) Регламентация работ по обеспечению безопасности автоматизированных систем.

Типовая лабораторная работа

Модуль 1. Общая характеристика информационной защиты автоматизированных систем.

Тема: Правовые основы обеспечения безопасности автоматизированных систем.

Цель: Практическое определение типа используемой информационной системы и выработка требований к обеспечению ее информационной безопасности.

Задание: Определить состав и **содержание** организационных и технических мер по обеспечению безопасности информации, обрабатываемой в информационной системе выбранной организации (торговое предприятие, ЗАГС, поликлиника).

Порядок выполнения:

1. Дополнительно изучить федеральное законодательство: Постановление Правительства РФ от 01.11.2012 № 1119 -«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных

системах», Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах», Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Определить тип обрабатываемой в выбранной автоматизированной системе информации.
3. Определить тип информационной системы и применяемое для данного типа федеральное законодательство.
4. В соответствие с выбранным типом, определить состав и содержание организационных и технических мер по обеспечению безопасности информации, обрабатываемой в информационной системе.
5. Ответить на контрольные вопросы:
   a) Приведите классификацию информации по доступности с точки зрения Федерального закона «Об информации, информационных технологиях и о защите информации».
   b) Дайте определение обладателя информации и оператора информационной системы.
   c) Перечислите права и обязанности обладателя информации.
   d) В каком кодексе предусмотрена ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)?
   e) Для кого аттестация ГИС по требованиям безопасности информации ФСТЭК России является обязательной?
   f) Когда проводится аттестация ГИС по требованиям безопасности информации ФСТЭК России?
   g) Перечислите классы защищенности СВТ в соответствии с руководящими документами ФСТЭК России.
   h) Перечислите классы защищенности АС в соответствии с руководящими документами ФСТЭК России.
   i) Какие подсистемы включает в себя комплекс программно-технических средств защиты информации от НСД в АС?
6. Защита лабораторной работы. Проводится в форме устного опроса после выполнения работы.

Критерии оценки лабораторной работы

Структура работы	Критерии оценки	Распределение баллов
Одно лабораторное задание	работа выполнена с ошибками и не получены ответы на все	2/5/10

	контрольные вопросы/ работа выполнена, но не получены ответы на все контрольные вопросы/ работа выполнена и получены ответы на все контрольные вопросы	

Типовое задание практического задания
Модуль 2. Методы, модели и механизмы обеспечения целостности и равномерной доступности данных
Построение системы защиты информации АС

Цель: практическое освоение материала дисциплины.

Задание: Создать комплексную систему защиты информации ограниченного доступа (персональных данных) АС условно существующей организации (на выбор: склад/юридическая фирма/торговая фирма/ЗАГС).

Аппаратура: Для выполнения лабораторной работы необходим персональный компьютер.

Программное обеспечение. Для выполнения лабораторной работы необходима операционная система с поддержкой графического окружения, установленный офисный пакет приложений, векторный графический редактор, редактор диаграмм и блок-схем.

Порядок выполнения:

1. Подготовить структурную схему информационной системы выбранной организации.
2. Подготовить схему размещения элементов информационной системы.
7. Определить тип информационной системы и перечень НПА федерального законодательства, применяемого для данной ИС.
8. Определить модель угроз для данной ИС.
9. Определить модель нарушителя.
10. Определить перечень требований организационных и технических мер для данной ИС.
11. Определить структурный состав системы защиты информации АС.
12. Защита практической работы. Проводится в форме устного опроса после выполнения работы.

Критерии оценки практической работы

Структура работы	Критерии оценки	Распределение баллов
Одно практическое задание	работа выполнена с ошибками/ работа выполнена, но без оптимизации схемы/ работа выполнена с оптимизацией схемы	0/3/5

Типовые вопросы теста

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

Необходимо выбрать один ответ из предложенных вариантов.

Модуль 1. Общая характеристика информационной защиты автоматизированных систем

Задание №1

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

а) Перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду;

б) анализ сетевого трафика;

в) перехват паролей;

г) реализация DDoS атак.

Задание №2

Идентификация и аутентификация субъектов и объект должна обеспечить:

а) проверку содержания инструкции пользователя ИС;

б) проверку целостности объектов доступа;

в) проверка принадлежности субъекту предъявленного им идентификатора;

г) проверку знания субъектом правил разграничения доступа.

Задание №3

Возможна ли реализация НДС через элементы информационной инфоструктуры, которые в процессе своего жизненного цикла оказываются за пределами контролируемой зоны:

а) да;

б) в обычных условиях;

в) в особых условиях;

г) нет.

Критерии оценки теста

Структура работы	Критерии оценки	Распределение баллов
Один тестовый вопрос (всего в тесте 25 вопросов) Тест (все 25 вопросов)	Не правильный ответ/ Правильный ответ	0/0,4 0/10

Типовые вопросы контрольной работы

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

Модуль 2. Методы, модели и механизмы обеспечения целостности и равномерной доступности данных

Вопросы контрольной работы:

1) Объясните концепцию монитора безопасности обращений.

2) Перечислите известные вам формальные модели управления доступом.

3) Объясните концепцию формальной модели управления доступом Харрисона-Руззо-Ульмана.

4) Опишите утечку права в модели Харрисона-Руззо-Ульмана.

5) Объясните концепцию формальной модели управления доступом Белла-ЛаПадулы.

6) Объясните концепцию формальной модели целостности Кларка-Вилсона.

7) Объясните концепцию формальной модели целостности Биба.

8) Объясните смысл схемы информационных потоков в формальной модели целостности Биба.

9) В чем суть совместного использования моделей Белла-ЛаПадулы и Биба.

10) Как звучит критерий безопасности системы при использовании ролевой модели.

Критерии оценки контрольной работы

Структура работы	Критерии оценки	Распределение баллов
Одно практическое задание	Работа не выполнена /работа выполнена неполно, не показано	0/13/25

	общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков/ работа выполнена в полном объеме и изложена грамотным языком в определенной логической последовательности с точным использованием специализированной терминологии; показано уверенное владение нормативной базой	

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Мельников В.П., Клейменов С.А., Петраков А.М.Информационная безопасность и защита информации: Учебное пособие. – М.: Академия. – 2011 с. https://bashedu.bibliotech.ru/Reader/Book/2013080217381731971500009579

2. Душкин А. В. , Ланкин О. В. , Потехецкий С. В. , Данилкин А. П. , Малышев А. А. Методологические основы построения защищенных автоматизированных систем: учебное пособие. -Воронеж: Воронежская государственная лесотехническая академия, 2013. – 258 с. http://biblioclub.ru/index.php?page=book&id=255851&sr=1

Дополнительная литература

3. Правовое обеспечение информационной безопасности: Учебное пособие. - М.: Маросейка, 2008. – 368 с. http://biblioclub.ru/index.php?page=book&id=96249&sr=1

4. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие. - М., Берлин: Директ-Медиа, 2015. – 253 с. http://biblioclub.ru/index.php?page=book&id=276557&sr=1

5. Анисимов А.А. Менеджмент в сфере информационной безопасности: Учебное пособие. - М.: Интернет-Университет Информационных Технологий, 2009. – 176 с. http://biblioclub.ru/index.php?page=book&id=232981&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 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2. *учебная аудитория для проведения лабораторных работ:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST - 1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV(XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт.	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.

аудитория № 420 (гуманитарный корпус), Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности аудитория №507 (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).	**Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 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.	

5. ***учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **6.** ***помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **7.*помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 523 (гуманитарный корпус).	**Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технические средства обработки информации, стенд "Устройство ПК". **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.	

Приложение 1

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

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины Информационная безопасность автоматизированных систем
на 7 семестр

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 ЗЕТ / 72 часов
Учебных часов на контактную работу с преподавателем:	54,2
лекций	18
практических/ семинарских	18
лабораторных	18
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	17,8
Учебных часов на подготовку к зачету	0

Форма контроля
Зачет 7 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛР	СР			
1	2	3	4	5	6	7	8	9
1	Модуль 1. Общая характеристика информационной защиты автоматизированных систем Тема: Место и роль автоматизированных систем в управлении бизнес-процессами. Защита автоматизированных систем как процесс управления рисками. Методы оценки целесообразности затрат на обеспечение безопасности. Особенности современных автоматизированных систем как объектов защиты. Определение безопасности автоматизированных систем. Информация и информационные ресурсы. Субъекты информационных отношений, их безопасность. Цель защиты автоматизированной системы и циркулирующей в ней информации. Тема: Уязвимость основных	2 2	2 2	 0	2 2	1- 5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	тестирование, практическое задание, контрольная работа, лабораторная работа

	структурно-функциональных элементов распределенных автоматизированных систем. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений. Классификация угроз безопасности.							
	Тема: Классификация каналов проникновения в автоматизированную систему и утечки информации. Неформальная модель нарушителя. Виды мер противодействия угрозам безопасности. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.	2	2	4	2			
	Тема: Защищаемая информация. Лицензирование. Сертификация средств защиты информации и аттестация объектов информатизации. Специальные требования и рекомендации по технической защите конфиденциальной информации. Юридическая значимость электронных документов с электронной подписью. Ответственность за нарушения в сфере защиты информации. Государственная система защиты информации. Контроль состояния защиты информации.	2	2	4	3			
2	Модуль 2. Методы, модели и механизмы обеспечения целостности и					1- 5	Самостоятельное изучение	тестирование, практическое

	правомерной доступности данных Тема: Технология управления безопасностью информации и ресурсов в автоматизированной системе. Институт ответственных за обеспечение информационной безопасности. Регламентация действий пользователей и обслуживающего персонала автоматизированной системы. Политика безопасности организации. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты. Распределение функций по обеспечению безопасности автоматизированных систем. Организационно-распорядительные документы по обеспечению безопасности автоматизированных систем. Тема: Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях. Регламентация правил парольной и антивирусной защиты. Регламентация порядка допуска к работе и изменения полномочий пользователей автоматизированной системы. Регламентация порядка изменения конфигурации аппаратно-программных средств автоматизированной системы. Регламентация процессов разработки,	2 2	2 2	 0	1,8 1		рекомендуемой основной и дополнительной литературы	задание, контрольная работа, лабораторная работа

	испытания, опытной эксплуатации, внедрения и сопровождения задач. Категорирование и документирование защищаемых ресурсов. Концепция информационной безопасности организации. План защиты информации. План обеспечения непрерывной работы и восстановления подсистем автоматизированной системы.							
	Тема: Основные механизмы защиты автоматизированных систем. Защита периметра компьютерных сетей и управление механизмами защиты. Страхование информационных рисков. Аппаратно-программные средства защиты информации от несанкционированного доступа. Средства аппаратной поддержки. Способы аутентификации. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа.	2	2	4	2			
	Тема: Защита от вмешательства в процесс нормального функционирования автоматизированной системы. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Защита данных от несанкционированной модификации, копирования и перехвата средствами	2	2	0	2			

	шифрования. Тема: Типовая корпоративная сеть. Уровни информационной инфраструктуры корпоративной сети. Уязвимости и их классификация. Классификация атак. Средства защиты сетей. Угрозы, связанные с периметром корпоративной сети. Составляющие защиты периметра. Межсетевые экраны. Анализ содержимого почтового и веб-трафика. Виртуальные частные сети. Управление уязвимостями. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования. Средства анализа защищенности системного уровня. Введение в управление журналами событий. Категории журналов событий. Инфраструктура управления журналами событий. Введение в технологию обнаружения атак. Классификация систем обнаружения атак.	2	2	6	2			
Всего:		18	18	18	17,8			

Приложение 2

Рейтинг-план дисциплины

Информационная безопасность автоматизированных систем

Направление 10.03.01 Информационная безопасность,
курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Общая характеристика информационной защиты автоматизированных систем				
Текущий контроль				25
1. Лабораторная работа	10	2	0	20
2. Практическая работа	5	1	0	5
Рубежный контроль				
Тест	25	1	0	25
Всего		3	0	50
Модуль 2. Методы, модели и механизмы обеспечения целостности и правомерной доступности данных				
Текущий контроль				25
1. Лабораторная работа	10	2	0	20
2. Практическая работа	5	1	0	5
Рубежный контроль				
1. Контрольная работа	25	1	0	25
Всего		4	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				
Зачет				
Итого				110