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.В.1.06 (вариативная)

Программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация
Технологии защиты информации в правоохранительной сфере

Квалификация
Специалист по защите информации

Разработчики (составители)
Старший преподаватель / Салов И.В.

Старший преподаватель, канд.хим.наук / Султанова А.А.

Для приема: 2016 г.

Уфа 2018 г.

Составители: И.В. Салов, А.А. Султанова

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

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

Заведующий кафедрой / Ф.И.О.

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

Заведующий кафедрой _____/ _____Ф.И.О/

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

Заведующий кафедрой _____/ _____Ф.И.О/

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

Заведующий кафедрой _____/ _____Ф.И.О/

Список документов и материалов

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

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	– Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1)	
	Знать типы технических и программно-аппаратных средств обработки и защиты информации	– Способность применять технические и программно-аппаратные средства обработки и защиты информации (ПК-2)	
	Знать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	– Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации (ПК-4)	
	Знать эксплуатационные и технико-экономические характеристики технических средств защиты информации и обеспечения информационной безопасности	– Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния (ПК-5)	
	Знать средства контроля контента	- Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности (ПК-22)	

	Знать наиболее распространенные методы и средства несанкционированного доступа к информации, методы и средства противодействия несанкционированному доступу к информации	– Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности (ПСК-1)	
Умения	Уметь обосновывать организационно-технические мероприятия по защите информации	– Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1)	
	Уметь выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	– Способность применять технические и программно-аппаратные средства обработки и защиты информации (ПК-2)	
	Уметь выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации	– Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации (ПК-4)	
	Уметь выполнять работы по установке, конфигурированию и эксплуатации компонентов технических систем обеспечения информационной безопасности и защиты информации	– Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния (ПК-5)	

	Уметь использовать базовые возможности информационных систем для решения задач фирмы	- Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности (ПК-22)	
	Уметь контролировать ход разработки проекта и осуществлять приемку комплекса	– Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности (ПСК-1)	
Владения (навыки / опыт деятельности)	Владеть навыками выявления и устранения угроз информационной безопасности	– Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз (ПК-1)	
	Владеть методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	– Способность применять технические и программно-аппаратные средства обработки и защиты информации (ПК-2)	
	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	– Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации (ПК-4)	
	Владеть методами оценки, тестирования. настройки и применения компонентов технических систем обеспечения защиты информации	– Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния (ПК-5)	
	Владеть навыками работы с компьютером как средством защиты	- Способность анализировать структуру и содержание информационных массивов и	

	информации	информационных процессов на предмет выявления угроз безопасности (ПК-22)	
	Владеть навыками нахождения и пресечения с помощью комплекса программно-аппаратных средств реальных и потенциальных каналов утечки информации на предприятии (организации, учреждении)	– Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности (ПСК-1)	

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

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

Дисциплина изучается на 4 курсе в 8-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 специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере специализации «Технологии защиты информации в правоохранительной сфере»: «Документоведение», «Информационная безопасность в правоохранительной сфере».

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

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

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)

Первый этап (уровень)	Знать политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	Не знает	Имеет фрагментарные знания о политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	Знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации, но допускает незначительные ошибки	Знает политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации
Второй этап (уровень)	Уметь обосновывать организационно-технические мероприятия по защите информации	Не умеет	Умеет обосновывать организационно-технические мероприятия по защите информации, но допускает существенные ошибки	Умеет обосновывать организационно-технические мероприятия по защите информации, но допускает незначительные ошибки	Умеет обосновывать организационно-технические мероприятия по защите информации
Третий этап (уровень)	Владеть навыками выявления и устранения угроз информационной безопасности	Не владеет	Недостаточно владеет навыками выявления и устранения угроз информационной безопасности	Владеет отдельными навыками выявления и устранения угроз информационной безопасности	Владеет навыками выявления и устранения угроз информационной безопасности

ПК-2: Способность применять технические и программно-аппаратные средства обработки и защиты информации

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 (уровень)	Знать типы технических и программно-аппаратных средств обработки и защиты информации	Не знает	Знает типы технических и программно-аппаратных средств обработки и защиты информации, допускает ошибки при определениях	Знает типы технических и программно-аппаратных средств обработки и защиты информации, допускает незначительные ошибки	Знает типы технических и программно-аппаратных средств обработки и защиты информации
Второй этап (уровень)	Уметь выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	Не умеет	Умеет выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации, но допускает неточности и ошибки	Уметь выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации, с допущением незначительных ошибок	Уметь выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации
Третий этап (уровень)	Владеть методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	Не владеет	Недостаточно владеет методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	Владеть методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации, но допускает ошибки	Владеть методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации

ПК-4: Способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного	Критерии оценивания результатов обучения			
		2 («Не	3	4 («Хорошо»)	5 («Отлично»)

	уровня освоения компетенций)	удовлетворительно»)	(«Удовлетворительно»)		
Первый этап (уровень)	Знать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	Не знает	Имеет фрагментарные знания о правовых нормах и стандартах по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	Знать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации, но допускает незначительные ошибки в определениях	Знать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации
Второй этап (уровень)	Уметь выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации	Не умеет	Допускает значительные ошибки при выборе типа необходимых средств для выявления наличия электронных средств перехвата информации	Допускает незначительные ошибки при выборе типа необходимых средств для выявления наличия электронных средств перехвата информации	Имеет навыки выбора типа необходимых средств для выявления наличия электронных средств перехвата информации
Третий этап (уровень)	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Не владеет	Недостаточно владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Владеет отдельными навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации

ПК-5: Способность осуществлять установку, настройку и эксплуатацию компонентов технических систем обеспечения безопасности информации и поддержку их работоспособного состояния

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 (уровень)	Знать эксплуатационные и технико-экономические характеристики технических средств защиты информации и обеспечения информационной безопасности	Не знает	Имеет фрагментарные знания об эксплуатационных и технико-экономических характеристиках технических средств защиты информации и обеспечения информационной безопасности	Знает основные эксплуатационные и технико-экономические характеристики технических средств защиты информации и обеспечения информационной безопасности	Знает эксплуатационные и технико-экономические характеристики технических средств защиты информации и обеспечения информационной безопасности
Второй этап (уровень)	Уметь выполнять работы по установке, конфигурированию и эксплуатации компонентов технических систем обеспечения информационной безопасности и защиты информации	Не умеет	Допускает значительные ошибки при работе по установке, конфигурированию и эксплуатации компонентов технических систем обеспечения информационной безопасности и защиты информации	Допускает незначительные ошибки при работе по установке, конфигурированию и эксплуатации компонентов технических систем обеспечения информационной безопасности и защиты информации	Уметь выполнять работы по установке, конфигурированию и эксплуатации компонентов технических систем обеспечения информационной безопасности и защиты информации
Третий этап (уровень)	Владеть методами оценки, тестирования. настройки и применения компонентов технических систем обеспечения защиты информации	Не владеет	Недостаточно владеет методами оценки, тестирования. настройки и применения компонентов технических систем обеспечения защиты информации	Владеет отдельными методами оценки, тестирования. настройки и применения компонентов технических систем обеспечения защиты информации	Владеет методами оценки, тестирования. настройки и применения компонентов технических систем обеспечения защиты информации

ПК-22: Способность анализировать структуру и содержание информационных массивов и информационных процессов на предмет выявления угроз безопасности.

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 (уровень)	Знать средства контроля контента	Не знает	Имеет фрагментарные знания о средствах контроля контента	Знает средства контроля контента, о допускает незначительные ошибки	Знает средства контроля контента
Второй этап (уровень)	Уметь использовать базовые возможности информационных систем для решения задач фирмы	Не умеет	Допускает значительные ошибки при использовании базовых возможностей информационных систем для решения задач фирмы	Уметь использовать базовые возможности информационных систем для решения задач фирмы, но допускает ошибки	Уметь использовать базовые возможности информационных систем для решения задач фирмы
Третий этап (уровень)	Владеть навыками работы с компьютером как средством защиты информации	Не владеет	Недостаточно владеет навыками работы с компьютером как средством защиты информации	Владеет отдельными навыками работы с компьютером как средством защиты информации	Владеет навыками работы с компьютером как средством защиты информации

ПСК-1: Способность участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности.

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 (уровень)	Знать наиболее распространенные методы и средства несанкционированного доступа к информации, методы и средства противодействия несанкционированному доступу к информации	Не знает	Имеет фрагментарные знания о наиболее распространенные методы и средства несанкционированного доступа к информации, методы и средства противодействия несанкционированному доступу к информации	Знает базовые методы и средства несанкционированного доступа к информации, методы и средства противодействия несанкционированному доступу к информации	Знает наиболее распространенные методы и средства несанкционированного доступа к информации, методы и средства противодействия несанкционированному доступу к информации
Второй этап (уровень)	Уметь контролировать ход разработки проекта и осуществлять приемку комплекса	Не умеет	Допускает значительные ошибки при осуществлении контроля хода разработки проекта	Умеет контролировать ход разработки проекта	Умеет контролировать ход разработки проекта и осуществлять приемку комплекса
Третий этап (уровень)	Владеть навыками нахождения и пресечения с помощью комплекса программно-аппаратных средств реальных и потенциальных каналов утечки информации на предприятии (организации, учреждении)	Не владеет	Недостаточно владеет навыками нахождения и пресечения с помощью комплекса программно-аппаратных средств реальных и потенциальных каналов утечки информации на предприятии (организации, учреждении)	Владеет отдельными навыками нахождения и пресечения с помощью комплекса программно-аппаратных средств реальных и потенциальных каналов утечки информации на предприятии (организации, учреждении)	Владеет навыками нахождения и пресечения с помощью комплекса программно-аппаратных средств реальных и потенциальных каналов утечки информации на предприятии (организации, учреждении)

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 политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации и оптимизации	ПК-1	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
	Знать типы технических и программно-аппаратных средств обработки и защиты информации	ПК-2	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
	Знать правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации	ПК-4	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
	Знать эксплуатационные и технико-экономические характеристики технических средств защиты информации и обеспечения информационной безопасности	ПК-5	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
	Знать средства контроля контента	ПК-22	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача

	Знать наиболее распространенные методы и средства несанкционированного доступа к информации, методы и средства противодействия несанкционированному доступу к информации	ПСК-1	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
2-й этап Уметь	Уметь обосновывать организационно-технические мероприятия по защите информации	ПК-1	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
	Уметь выполнять работы по установке, конфигурированию и эксплуатации технических и программных средств обеспечения информационной безопасности и защиты информации	ПК-2	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
	Уметь выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации	ПК-4	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
	Уметь выполнять работы по установке, конфигурированию и эксплуатации компонентов технических систем обеспечения информационной безопасности и защиты информации	ПК-5	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
	Уметь использовать базовые возможности информационных систем для решения задач фирмы	ПК-22	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача

	Уметь контролировать ход разработки проекта и осуществлять приемку комплекса	ПСК-1	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
3-й этап Владеть	Владеть навыками выявления и устранения угроз информационной безопасности	ПК-1	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
	Владеть методами оценки, тестирования. настройки на применение средств программно-технического обеспечения защиты информации	ПК-2	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
	Владеть навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации	ПК-4	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
	Владеть методами оценки, тестирования. настройки и применения компонентов технических систем обеспечения защиты информации	ПК-5	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
	Владеть навыками работы с компьютером как средством защиты информации	ПК-22	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача
	Владеть навыками нахождения и пресечения с помощью комплекса программно-аппаратных средств реальных и потенциальных каналов утечки информации на предприятии (организации,	ПСК-1	тестирование, практическое задание, защита практической работы, творческое задание (презентация, доклад), контрольная работа, задача

	учреждении)		

Экзамен

Экзамен является оценочным средством для всех этапов освоения компетенции.

Структура экзаменационного билета

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

Типовые экзаменационные материалы

Типовые экзаменационные вопросы:

1. Особенности современных автоматизированных систем как объектов защиты.
2. Основные понятия в области безопасности автоматизированных систем
3. Определение безопасности автоматизированных систем.
4. Информация и информационные ресурсы.
5. Субъекты информационных отношений, их безопасность.
6. Цель защиты автоматизированной системы и циркулирующей в ней информации.
7. Угрозы безопасности автоматизированных систем
8. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем.
9. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений.
10. Классификация угроз безопасности.
11. Классификация каналов проникновения в автоматизированную систему и утечки информации.
12. Неформальная модель нарушителя.
13. Меры и основные принципы обеспечения безопасности автоматизированных систем
14. Виды мер противодействия угрозам безопасности.
15. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.
16. Правовые основы обеспечения безопасности автоматизировании систем
17. Защищаемая информация.
18. Лицензирование.
19. Сертификация средств защиты информации и аттестация объектов информатизации.
20. Специальные требования и рекомендации по технической защите конфиденциальной информации.
21. Юридическая значимость электронных документов с электронной подписью.
22. Ответственность за нарушения в сфере защиты информации.
23. Государственная система защиты информации
24. Главные направления работ по защите информации.
25. Структура государственной системы защиты информации.

26. Организация защиты информации в системах и средствах информатизации и связи.
27. Контроль состояния защиты информации.
28. Финансирование мероприятий по защите информации.
29. Организационная структура системы обеспечения безопасности автоматизированных систем
30. Технология управления безопасностью информации и ресурсов в автоматизированной системе.
31. Институт ответственных за обеспечение информационной безопасности.
32. Регламентация действий пользователей и обслуживающего персонала автоматизированной системы.
33. Политика безопасности организации.
34. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты.
35. Распределение функций по обеспечению безопасности автоматизированных систем.
36. Организационно-распорядительные документы по обеспечению безопасности автоматизированных систем.
37. Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях
38. Проблема человеческого фактора.
39. Общие правила обеспечения безопасности.
40. Обязанности ответственного за обеспечение безопасности информации в подразделении.
41. Ответственность за нарушения требований обеспечения безопасности.
42. Порядок работы с носителями ключевой информации.
43. Регламентация работ по обеспечению безопасности автоматизированных систем
44. Регламентация правил парольной и антивирусной защиты.
45. Регламентация порядка допуска к работе и изменения полномочий пользователей автоматизированной системы.
46. Регламентация порядка изменения конфигурации аппаратно-программных средств автоматизированной системы.
47. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач.
48. Категорирование и документирование защищаемых ресурсов ....
49. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов.
50. Категорирование защищаемых ресурсов.
51. Проведение информационных обследований и документирование защищаемых ресурсов.
52. Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем автоматизированной системы.
53. Концепция информационной безопасности организации.
54. План защиты информации.
55. План обеспечения непрерывной работы и восстановления подсистем автоматизированной системы.
56. Назначение и возможности средств защиты информации от несанкционированного доступа.
57. Основные механизмы защиты автоматизированных систем.
58. Защита периметра компьютерных сетей и управление механизмами защиты.

59. Страхование информационных рисков.
60. Аппаратно-программные средства защиты информации от несанкционированного доступа.
61. Рекомендации по выбору средств защиты информации от несанкционированного доступа.
62. Обзор существующих на рынке средств защиты информации от несанкционированного доступа.
63. Средства аппаратной поддержки.
64. Способы аутентификации.
65. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа
66. Стратегия безопасности Microsoft.
67. Защита от вмешательства в процесс нормального функционирования автоматизированной системы.
68. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы.
69. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа.
70. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.
71. Обеспечение безопасности компьютерных сетей.
72. Проблемы обеспечения безопасности в компьютерных сетях.
73. Типовая корпоративная сеть.
74. Уровни информационной инфраструктуры корпоративной сети.
75. Уязвимости и их классификация.
76. Классификация атак.
77. Средства защиты сетей.
78. Защита периметра корпоративной сети.
79. Угрозы, связанные с периметром корпоративной сети.
80. Составляющие защиты периметра.
81. Межсетевые экраны.
82. Анализ содержимого почтового и веб-трафика.
83. Виртуальные частные сети.
84. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности.
85. Управление уязвимостями.
86. Архитектура систем управления уязвимостями.
87. Особенности сетевых агентов сканирования.
88. Средства анализа защищенности системного уровня.
89. Мониторинг событий безопасности
90. Введение в управление журналами событий.
91. Категории журналов событий.
92. Инфраструктура управления журналами событий.
93. Введение в технологию обнаружения атак.
94. Классификация систем обнаружения атак.

Пример экзаменационного билета:

Форма 1.4.-33

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

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Дисциплина Информационная безопасность автоматизированных систем

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Классификация компьютерных вирусов
2. Межсетевые экраны: определение, функции

Зав. Кафедрой УИБ А.С. Исмагилова

2018-2019 учебный год
Кафедра управления информационной безопасностью

Критерии оценивания результатов экзамена для ОФО:

Критерии оценки (в баллах):

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

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

- 10-16 баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос.

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

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

Экзамены:

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

Тестирование
Модуль 1

Задание №1 (***Образец***)

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.

Задание №4

Одним из условий реализации DDoS атак является:

а) выполнение атаки с одного компьютера;

б) выполнение атаки из внешней сети;

в) выполнение атаки из внутренней сети;

г) выполнение атаки большим количеством компьютеров.

Задание № 5

Одним из основных условий реализации угроз непосредственного доступа в операционную среду компьютера является:

а) наличие сетевого сканера;

б) физический доступ нарушителя к компьютеру;

в) физический доступ в помещение с компьютером;

г) удаленный доступ нарушителя к компьютеру.

Критерии оценки теста

Структура работы	Критерии оценки	Распределение баллов
Один тестовый вопрос (всего в тесте 15 вопросов)	Правильный ответ/не правильный ответ	1/0

Лабораторная работа

Темы лабораторных заданий

1. Защищаемая информация.
2. Построение системы защиты информации АС.
3. Способы аутентификации.
4. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы.

Модуль 1, 2

Тема: Построение системы защиты информации АС.

Цель: Отработка на практике методики построения защиты АС.

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.

Критерии оценки лабораторной работы

Структура работы	Критерии оценки	Распределение баллов
Одна лабораторная работа	работа выполнена с ошибками/ работа выполнена, но без оптимизации схемы/ работа выполнена с оптимизацией схемы	2/4/7

Творческое задание (презентация, доклад)
Модуль 1, 2

Выполняется по результатам изучения темы дисциплины с целью дополнения практического материала.

Примеры тем творческих заданий

Построение систем защиты от угроз нарушения конфиденциальности информации.
Межсетевое экранирование.
Методы защиты внешнего периметра.
Построение систем защиты от угроз нарушения целостности.

Критерии оценки творческой работы

Структура работы	Критерии оценки	Распределение баллов
Одно практическое задание	Задание не выполнено / отсутствует логичность изложения информации / логичное изложения информации	0/1/3

Контрольная работа
Модуль 1, 2

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 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	0/3/5

Практическая работа

Цифровая подпись

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

Что такое цифровая подпись. Изобразите схему реализации цифровой подписи с подробным описанием каждого этапа.

Критерии и методика оценивания:

- 5 баллов выставляется студенту, если составлен правильный алгоритм решения задачи, в логическом рассуждении, в выборе формул и решении нет ошибок, получен верный ответ, задача решена рациональным способом, показано уверенное владение нормативной базой;

- 4 балла выставляется студенту, если составлен правильный алгоритм решения задачи, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задача решена нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ, нет определенной логической последовательности, неточно используется специализированная терминология;

- 3 балла выставляется студенту, если в логическом рассуждении нет существенных ошибок, но допущены существенные ошибки в выборе формул или в математических расчетах; задача решена не полностью или в общем виде;

- 2 балла выставляется студенту, если задача решена неправильно.

4.3. Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 2.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

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

Дополнительная литература

1. Сердюк В.А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных систем предприятий. - М.: НИУ Высшая школа экономики, 2011. – 574 с. http://biblioclub.ru/index.php?page=book&id=74298&sr=1
2. 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
3. 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
4. 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
5.

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*:** Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (гуманитарный корпус). **3. *учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус),	Лекции, лабораторные и практические занятия, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ MA1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-

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 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		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. **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.

(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).		

Приложение 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины Информационная безопасность автоматизированных систем на 8 семестр
ОФО

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часов
Учебных часов на контактную работу с преподавателем:	49,2
лекций	16
практических/ семинарских	16
лабораторных	16
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	42
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	52,8

Форма (ы) контроля:

экзамен 8 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛР	СР			
1	2	3	4	5	6	7	8	9
1	Общая характеристика информационной защиты автоматизированных систем Тема: Особенности современных автоматизированных систем как объектов защиты. Основные понятия в области безопасности автоматизированных систем. Определение безопасности автоматизированных систем. Информация и информационные ресурсы. Субъекты информационных отношений, их безопасность. Цель защиты автоматизированной системы и циркулирующей в ней информации. Угрозы безопасности автоматизированных систем. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений. Классификация угроз безопасности. Классификация каналов проникновения в автоматизированную систему и утечки информации. Неформальная модель нарушителя. Меры и основные принципы обеспечения безопасности автоматизированных систем. Виды мер противодействия угрозам безопасности. Принципы построения системы обеспечения безопасности информации в автоматизированной системе. Тема: Правовые основы обеспечения безопасности автоматизировании систем. Защищаемая информация. Лицензирование. Сертификация средств защиты информации и аттестация объектов информатизации.	2 2	4	4	5 5	1- 4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	тестирование, практическое задание, защита практической работы, творческое задание, контрольная работа

	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. Главные направления работ по защите информации. Структура государственной системы защиты информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации. Финансирование мероприятий по защите информации.							
	Тема: Организационная структура системы обеспечения безопасности автоматизированных систем. 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. Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях. Проблема человеческого фактора. Общие правила обеспечения безопасности. Обязанности ответственного за обеспечение безопасности информации в подразделении. Ответственность за нарушения требований обеспечения безопасности. Порядок работы с носителями ключевой информации.	2			5			
	Тема: Регламентация работ по обеспечению безопасности автоматизированных систем. 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, испытания, опытной эксплуатации, внедрения и сопровождения задач. Категорирование и документирование защищаемых ресурсов. Определение	2	4	4	6			

	градаций важности и соответствующих уровней обеспечения защиты ресурсов. Категорирование защищаемых ресурсов. Проведение информационных обследований и документирование защищаемых ресурсов. Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем автоматизированной системы. Концепция информационной безопасности организации. План защиты информации. План обеспечения непрерывной работы и восстановления подсистем автоматизированной системы.							
2	Методы, модели и механизмы обеспечения целостности и правомерной доступности данных Тема: Назначение и возможности средств защиты информации от несанкционированного доступа. Основные механизмы защиты автоматизированных систем. Защита периметра компьютерных сетей и управление механизмами защиты. Страхование информационных рисков. Аппаратно-программные средства защиты информации от несанкционированного доступа. Рекомендации по выбору средств защиты информации от несанкционированного доступа. Обзор существующих на рынке средств защиты информации от несанкционированного доступа. Средства аппаратной поддержки. Способы аутентификации. Тема: Применение штатных и дополнительных средств защиты информации от несанкционированного доступа. Стратегия безопасности Microsoft. Защита от вмешательства в процесс нормального функционирования автоматизированной системы. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования. Тема: Обеспечение безопасности компьютерных сетей. Проблемы обеспечения безопасности в компьютерных сетях. Типовая корпоративная сеть. Уровни информационной инфраструктуры корпоративной сети. Уязвимости и их классификация. Классификация атак. Средства защиты сетей. Защита периметра корпоративной	2 2 2	4 4	4 4	5 5 5	1- 4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическое задание, защита практической работы, творческое задание, контрольная работа, задача

	сети. Угрозы, связанные с периметром корпоративной сети. Составляющие защиты периметра. Межсетевые экраны. Анализ содержимого почтового и веб-трафика. Виртуальные частные сети. Тема: Обнаружение и устранение уязвимостей. Возможности сканеров безопасности. Управление уязвимостями. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования. Средства анализа защищенности системного уровня. Мониторинг событий безопасности Введение в управление журналами событий. Категории журналов событий. Инфраструктура управления журналами событий. Введение в технологию обнаружения атак. Классификация систем обнаружения атак.	2			6			
	Всего часов	16	16	16	42			

Приложение 2

Рейтинг-план дисциплины

Информационная безопасность автоматизированных систем

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере, курс 4, семестр 8

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1.				
Текущий контроль				
1. Творческое задание	3	1	0	3
2. Контрольная работа	5	1	0	5
3. Практическая работа	7	1	0	7
Рубежный контроль				
Тест	15	1	0	15
Всего		16	0	30
Модуль 2.				
Текущий контроль				
1. Творческое задание	3	1	0	3
2. Контрольная работа	5	1	0	5
3. Практическая работа	7	1	0	7
Рубежный контроль				
1. Задача	5	5	0	25
Всего		7	0	40
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10
Итоговый контроль				
1. Экзамен	30	1	0	30