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

Утверждено:
на заседании кафедры
протокол № 8 от «24» февраля 2021 г.

Зав. кафедрой _____ /Исмагилова А.С.

Согласовано:
Председатель УМК института

_____/Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина
Защищенные информационные системы

обязательная часть

программа магистратуры

Направление подготовки
10.04.01 Информационная безопасность

Направленность подготовки
Информационная безопасность цифровых технологий

Квалификация
магистр

Разработчик (составитель)
доцент кафедры, к. филос. н.

_____ / Миронова Н.Г.

Для приема: 2021 г.

Уфа 2021 г.

Составитель: к.филос.н. Миронова Наталия Геннадьевна

Рабочая программа дисциплины утверждена на заседании кафедры протокол от «24» февраля 2021 № 8

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

Заведующий кафедрой / Исмагилова А.С. /

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

Заведующий кафедрой _____/ Исмагилова А.С. /

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций *(при наличии ОПК)*	**Формируемая компетенция (с указанием кода)**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения по дисциплине**
	ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.	ОПК-1.1. Знает основные требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС.	Знать нормативную базу, регламентирующую создание и эксплуатацию ИАС (требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС); знать назначение и классификацию информационных и аналитических систем, систем управления; иметь представления о содержании инструкций по организации обследования автоматизируемых подразделений; знать специфические особенности функционирования подразделений, подлежащих автоматизации.
		ОПК-1.2. Умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	Уметь разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ. Уметь производить изучение служебной деятельности автоматизируемых подразделений.
		ОПК-1.3. Владеет основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Владеть основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта. Владеть навыками реализации типовых методик изу-

			чения служебной деятельности автоматизируемых подразделений; владеть навыком изучения процессов функционирования автоматизируемых подразделений в целях определения их информационных потребностей
	ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	ОПК-2.1. Знает основные требования к техническому проекту подсистемы либо компонента системы обеспечения информационной безопасности; состав/архитектуру СОИБ и процедуру создания СОИБ, этапы проектирования СОИБ. Знает состав технического проекта системы/подсистемы информационной безопасности, порядок его подготовки.	Знать структуры функциональной и обеспечивающих частей ИАС, методы проведения предпроектного обследования при разработке ИАС. Знать основные требования к техническому проекту подсистемы либо компонента системы обеспечения информационной безопасности; состав/архитектуру СОИБ и процедуру создания СОИБ, этапы проектирования СОИБ. Знать состав технического проекта системы/подсистемы информационной безопасности, порядок его подготовки.
		ОПК-2.2. Умеет выполнять обследование/аудит и моделирование предметной области, моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Уметь выполнять обследование/аудит и моделирование предметной области, моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности. Выявлять информационные потребности автоматизируемых подразделений Производить формализацию предметной области с целью создания ИАС Составлять техническое задание на разработку ИАС Готовить проектную документацию на создаваемые ИАС
		ОПК-2.3. Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.	Владеть основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи. Владеть навыками подготовки проектов нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации ИАС

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Защищенные информационные системы» относится к обязательной части.

Дисциплина изучается на 1 курсе магистратуры в 1 и 2 семест*рах.*

Цели изучения дисциплины: изучение методики анализа угроз при разработке и эксплуатации защищенных информационных систем; методик оценки рисков ИБ на объекте информатизации; концептуального проектирования защищенных систем обработки информации; требований к уровню и средствам защиты информации в ИС на основе отечественных и международных стандартов; получение знаний и навыков по технологиям обеспечения защиты информации в информационных системах (в т.ч. ЗИС)

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 и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.

Для зачета:

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ОПК-1.1. Знает основные требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС.	Знать нормативную базу, регламентирующую создание и эксплуатацию ИАС (требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС); знать назначение и классификацию информационных и аналитических систем, систем управления; иметь представления о содержании инструкций по организации обследования автоматизируемых подразделений; знать специфические особенности функционирования подразделений, подлежащих автоматизации.	Незнание или очень слабое знание указанных нормативном базы, требований стандартов	Продемонстрировано знание
ОПК-1.2. Умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств	Уметь разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ. Уметь производить изучение служебной деятельности автоматизируемых подразделений.	Неполное умение, фрагментарные навыки	В целом сформировавшееся умение.

СОИБ); способен обосновать требования к СОИБ.			
ОПК-1.3. Владеет основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Владеть основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта. Владеть навыками реализации типовых методик изучения служебной деятельности автоматизируемых подразделений; владеть навыком изучения процессов функционирования автоматизируемых подразделений в целях определения их информационных потребностей	Неполное владение указанными методами и навыками	В целом сформировавшееся владение указанными методиками и навыками

Для экзамена:

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ОПК-1.1. Знает основные требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС.	Знать нормативную базу, регламентирующую создание и эксплуатацию ИАС (требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС); знать назначение и классификацию информационных и аналитических систем, систем управления; иметь представления о содержании инструкций по организации обследования автоматизируемых подразделений; знать специфические особенности функционирования подразделений, подлежащих автоматизации.	Не знает	Слабо знает указанные требования и технологии, имеет фрагментарные знания.	Демонстрирует хорошее знание указанных требований и технологий, но не всегда способен увязать их с практикой управления службой защиты информации.	Демонстрирует целостные, системные знания в указанной сфере.
ОПК-1.2. Умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприя-	Уметь разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий	Не умеет	Слабо демонстрирует указанные умения и знания, без связи навыка-	Демонстрирует хорошее теоретическое знание компетенции, но	Демонстрирует уверенное, свободное владение указанными

тий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ. Уметь производить изучение служебной деятельности автоматизируемых подразделений.		ми решения задач организации службы защиты информации.	недостаточное владение практической стороной при решении задач организации службы защиты информации	навыками при решении задач организации службы защиты информации
ОПК-1.3. Владеет основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Владеть основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта. Владеть навыками реализации типовых методик изучения служебной деятельности автоматизируемых подразделений; владеть навыком изучения процессов функционирования автоматизируемых подразделений в целях определения их информационных потребностей	Не владеет	Слабо демонстрирует указанные навыки.	Демонстрирует хорошее владение компетенцией, но имеет устаревшие и малоактуальные сведения.	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации.

ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.

Для зачета:

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ОПК-2.1. Знает основные требования к техническому проекту подсистемы либо компонента системы обеспечения информационной безопасности; состав/архитектуру СОИБ и процедуру создания СОИБ, этапы проектирования СОИБ. Знает состав технического проекта системы/подсистемы информационной безопасности, порядок его подготовки.	Знать структуры функциональной и обеспечивающих частей ИАС, методы проведения предпроектного обследования при разработке ИАС. Знать основные требования к техническому проекту подсистемы либо компонента системы обеспечения информационной безопасности; состав/архитектуру СОИБ и процедуру создания СОИБ, этапы проектирования СОИБ. Знать состав технического проекта системы/подсистемы информационной безопасности, порядок его подготовки.	Незнание или очень слабое знание указанных нормативном базы, требований стандартов	Продемонстрировано знание
ОПК-2.2. Умеет выполнять обследование/аудит и моделирование предметной области, моделиро-	Уметь выполнять обследование/аудит и моделирование предметной области, моделировать угрозы информацион-	Неполное умение, фрагментарные навыки	В целом сформировавшееся

вать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности. Выявлять информационные потребности автоматизируемых подразделений Производить формализацию предметной области с целью создания ИАС Составлять техническое задание на разработку ИАС Готовить проектную документацию на создаваемые ИАС		умение.
ОПК-2.3. Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.	Владеть основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи. Владеть навыками подготовки проектов нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации ИАС	Неполное владение указанными методами и навыками	В целом сформировавшееся владение указанными методиками и навыками

Для экзамена:

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ОПК-2.1. Знает основные требования к техническому проекту подсистемы либо компонента системы обеспечения информационной безопасности; состав/архитектуру СОИБ и процедуру создания СОИБ, этапы проектирования СОИБ. Знает состав технического проекта системы/подсистемы информационной безопасности, порядок его подготовки.	Знать структуры функциональной и обеспечивающих частей ИАС, методы проведения предпроектного обследования при разработке ИАС. Знать основные требования к техническому проекту подсистемы либо компонента системы обеспечения информационной безопасности; состав/архитектуру СОИБ и процедуру создания СОИБ, этапы проектирования СОИБ. Знать состав технического проекта системы/подсистемы информационной безопасности, порядок его подготовки.	Не знает	Слабо знает указанные требования и технологии, имеет фрагментарные знания.	Демонстрирует хорошее знание указанных требований и технологий, но не всегда способен увязать их с практикой управления службой защиты информации.	Демонстрирует целостные, системные знания в указанной сфере.
ОПК-2.2. Умеет выполнять обследование/аудит и моделирование предметной области, моделировать угрозы информационной безопасности; умеет обосновывать тре-	Уметь выполнять обследование/аудит и моделирование предметной области, моделировать угрозы информационной безопасности; умеет обосновывать требования к	Не умеет	Слабо демонстрирует указанные умения и знания, без связи навыками решения задач организации службы	Демонстрирует хорошее теоретическое знание компетенции, но недостаточное владение практической	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации

бования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности	техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности. Выявлять информационные потребности автоматизируемых подразделений Производить формализацию предметной области с целью создания ИАС Составлять техническое задание на разработку ИАС Готовить проектную документацию на создаваемые ИАС		защиты информации.	стороной при решении задач организации службы защиты информации	службы защиты информации
ОПК-2.3. Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.	Владеть основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи. Владеть навыками подготовки проектов нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации ИАС	Не владеет	Слабо демонстрирует указанные навыки.	Демонстрирует хорошее владение компетенцией, но имеет устаревшие и малоактуальные сведения.	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации.

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине

ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ОПК-1.1. Знает основные требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС.	Знать нормативную базу, регламентирующую создание и эксплуатацию ИАС (требования к системе обеспечения информационной безопасности; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования стандартов к разработке и эксплуатации ИС/АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС); знать назначение и классификацию информационных и аналитических систем, систем управления; иметь представления о содержании инструкций по организации обследования автоматизируемых подразделений; знать	практические задания; отчет по практикам); опрос/доклад; компьютерный тест

	специфические особенности функционирования подразделений, подлежащих автоматизации.	
ОПК-1.2. Умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	Уметь разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ. Уметь производить изучение служебной деятельности автоматизируемых подразделений.	практические задания; отчет по практикам); компьютерный тест
ОПК-1.3. Владеет основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Владеть основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта. Владеть навыками реализации типовых методик изучения служебной деятельности автоматизируемых подразделений; владеть навыком изучения процессов функционирования автоматизируемых подразделений в целях определения их информационных потребностей	практические задания; отчет по практикам);

ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ОПК-2.1. Знает основные требования к техническому проекту подсистемы либо компонента системы обеспечения информационной безопасности; состав/архитектуру СОИБ и процедуру создания СОИБ, этапы проектирования СОИБ. Знает состав технического проекта системы/подсистемы информационной безопасности, порядок его подготовки.	Знать структуры функциональной и обеспечивающих частей ИАС, методы проведения предпроектного обследования при разработке ИАС. Знать основные требования к техническому проекту подсистемы либо компонента системы обеспечения информационной безопасности; состав/архитектуру СОИБ и процедуру создания СОИБ, этапы проектирования СОИБ. Знать состав технического проекта системы/подсистемы информационной безопасности, порядок его подготовки.	практические задания; отчет по практикам); опрос/доклад; компьютерный тест
ОПК-2.2. Умеет выполнять обследование/аудит и моделирование предметной области, моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Уметь выполнять обследование/аудит и моделирование предметной области, моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности. Выявлять информационные потребности автоматизируемых подразделений Производить формализацию предметной области с целью создания ИАС Составлять техническое задание на разработку ИАС Готовить проектную документацию на создаваемые ИАС	практические задания; отчет по практикам); компьютерный тест
ОПК-2.3. Владеет основными навыками использования технологий, методов и средств тех-	Владеть основными навыками использования технологий, методов и средств технического проектирования и моделирования	практические задания; отчет по практикам);

нического проектирования и моделирования СОИБ с учетом поставленной задачи.	СОИБ с учетом поставленной задачи. Владеть навыками подготовки проектов нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации ИАС	

Критериями оценивания при модульно-рейтинговой системе являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения разделов № 1-2 дисциплины, перечисленных в рейтинг-плане дисциплины.

Для зачета (в 1 семестре): текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания для зачета:

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

не зачтено – от 0 до 59 рейтинговых баллов).

Критериями оценивания при модульно-рейтинговой системе являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения разделов № 3-4 дисциплины, перечисленных в рейтинг-плане дисциплины.

Для экзамена (во 2 семестре): текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10;

Шкалы оценивания для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

Рейтинг – план дисциплины
«Защищенные информационные системы»

Направление подготовки 10.04.01 Информационная безопасность

курс 1, семестр 1

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль (Раздел) 1				
Текущий контроль				
Аудиторная работа				**12,5**
1. Доклады/ практические задания	**5**	**2**	**0**	10
2. Лабораторные задания	**2,5**	**1**	**0**	2,5
Рубежный контроль				**7,5**
1. Отчет по лабораторным работам	**7,5**	**1**	**0**	7,5
Модуль (Раздел) 2				
Текущий контроль				
Аудиторная работа				**37,5**
1. Доклады/ практические задания	**5**	**6**	**0**	30
2. Лабораторные задания	**2,5**	**3**	**0**	7,5
Рубежный контроль				**42,5**
1. Отчет по лабораторным работам	**7,5**	**3**	**0**	22,5
2. Тест итоговый (зачетный)	**0,83**	**24**	**0**	20
Поощрительные баллы				
1. Студенческая олимпиада				5
2. Публикация статей				5
3. Работа со школьниками (кружок, конкурсы, олимпиады)				
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				

Рейтинг – план дисциплины
«Защищенные информационные системы»

Направление подготовки 10.04.01 Информационная безопасность

курс 1, семестр 2

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль (Раздел) 3				
Текущий контроль				**12**
Аудиторная работа				
1. Практические занятия	**3**	**4**	**0**	12
Рубежный контроль				**10**
1. Отчет по лабораторным работам	10	1	0	10
Модуль (Раздел) 4				
Текущий контроль				**28**
Аудиторная работа				
1. Практические задания	**3**	**4**	**0**	12
1. Отчет по лабораторным работам	**8**	**2**	**0**	16
Рубежный контроль				**20**
1. Отчет по лабораторным работам *(или тест итоговый)*	**5**	**1**	**0**	5
2. Курсовой проект	**1**	**15**		15
Поощрительные баллы				
1. Студенческая олимпиада				**0**
2. Публикация статей				**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				
Экзамен				**30**

Экзаменационные билеты

Структура экзаменационного билета:

Экзаменационный билет содержит 2 теоретических вопроса из нижеприведенного перечня.

Перечень вопросов для экзамена:

1. Угрозы и риски информационной безопасности, связанные с использованием информационных систем.
2. Понятие защищенной информационной системы. Области применения защищенных ИС. Примеры защищенных ИС.
3. Методы хранения данных при реализации ЗИС. СУБД для организации защищенных ИС. Встроенные инструменты защиты данных в СУБД (с учетом модели организации данных).
4. Штатные и добавленные средства и способы программной реализации защиты информации (на конкретных примерах).
5. Методологии проектирования ИС. Принципы проектирования и разработки ЗИС.
6. Этапы проектирования и создания защищенной информационной системы.
7. Этапы создания системы защиты информационной системы.
8. Стандарты и нормативные документы, регламентирующие создание АС в защищенном исполнении
9. Стандарты и нормативные документы, регламентирующие построение системы защиты для информационной системы
10. Возможные уязвимости информационной безопасности для ИС и меры по их снижению, реализуемые на этапе разработки ИС.
11. Требования нормативных документов ФСТЭК, ФСБ и др. отечественных регуляторов к уровню защищенности информационных систем различных классов (на конкретных примерах классов ИС).
12. Классификация информационных систем. Нормативные документы, порядок определения класса защищенности ИС.
13. Программно-аппаратные средства защиты информации. Проблема интеграция средств защиты и компонентов информационных систем при проектировании СЗИ ИС (или ЗИС).
14. Роль специалиста по информационной безопасности в разработке, модернизации, внедрении ИС, в т.ч. защищенных ИС.
15. Этапы разработки информационных систем. Язык нотаций UML и виды диаграмм и моделей, используемые для проектирования ИС
16. Сценирование (описание сценариев) актуальных угроз ИБ, согласно методике ФСТЭК: исходные данные для сценирования, элементы сценария угроз, инструменты для описания сценария.
17. Методологии моделирования критических информационных/рабочих процессов (idef0, dfd, idef3, bpmn, flow chart и др.). Входные и выданные данные для построения модели.
18. Задачи обеспечения ИБ, угрозы ИБ, источники уязвимостей ИС. Способы, средства выявления и оценки уязвимостей ИС.
19. Требования к уровню защищенности ИС и обрабатываемой в них информации, в зависимости от уровня конфиденциальности и критичности информации.
20. Меры и подходы к обеспечению защищенности ИС на этапах разработки.
21. Проектирование СЗИ для ИС (этапы). Технические средства защиты информации в ИС.
22. ГИС и требования ФСТЭК и ФСБ к их уровню защищенности
23. ИСПДн и требования ФСТЭК и ФСБ к их уровню защищенности
24. АИС, АСУ и требования ФСТЭК и ФСБ к их уровню защищенности

25. ИС реального времени и требования к надежности таких ИС.
26. Особенности построения СЗИ для обработки ИСПДн
27. Угрозы для ИСПДн. Нормативные документы регуляторов в области требований к обеспечению защищенности ПДн..
28. Особенности построения СЗИ для обработки ГИС
29. Особенности построения СЗИ для обработки информации, содержащей коммерческую и служебную тайны.
30. Особенности построения СЗИ для обработки информации, содержащей государственную тайну.
31. Принципы организации документирования разработки, процесса сопровождения программного обеспечения.
32. Функциональные возможности современных систем управления базами данных в части средств защиты. Архитектура, основные модели, последовательность и содержание этапов проектирования, физическая организация баз данных. Основные модели данных, модели представления знаний и программные средства работы с ними. Инфологическая модель предметной области.
33. Проектирование, документирование, разработке, тестирование и отладка компонентов обеспечивающей части ИАС при разработке ЗИС/ЗАС. Принципы организации документирования разработки, процесса сопровождения программного обеспечения.
34. Показатели качества и надежности ИС в защищенном исполнении и методы реализации принципов надежности и защищенности. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.
35. Особенности защиты информации в АСУ. Исследование аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем. Исследование программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах
36. Разработка технического задания на проектирование ЗИС/ЗАС: Подготовка проектов нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации ИАС. Подготовка проектной документации на создаваемые ИАС. Проведение технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы.
37. Разработка технического задания на проектирование ЗИС/ЗАС: Формирование основных показателей и критериев эффективности ИАС. Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем. Формирование конфигурации и состава обеспечивающей части ИАС.
38. Разработка технического задания на проектирование ЗИС/ЗАС: Формирование функциональной части ИАС. Формирование технологии функционирования ИАС. Формирование требований по защите информации, включая использование математического аппарата для решения прикладных задач.
39. Проектирование технического обеспечения защищенной ИС/АС: разработка аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем. Проектная и эксплуатационная документация на систему защиты информации.
40. Проектирование технического обеспечения защищенной ИС/АС: составление методик тестирования систем защиты информации автоматизированных систем. Определение комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в ИС; состав комплекса средств защиты информации в ИАС.
41. Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах. Обоснование необходимости использования криптографических средств защиты информации.
42. Принципы эксплуатации и сопровождения ЗИС. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты

информации. Технико-экономическое обоснование проектных решений обеспечения защиты информации в ИС для обеспечения требуемого уровня защищенности.

43. Эксплуатация ЗИС: администрирование ЗИС. Доступ к данным безопасности. Монитор безопасности, протоколирование, аудит, шифрование, контроль целостности данных, использование электронной цифровой подписи.
44. Документирование ЗИС: перечень нормативно-распорядительных документов (приказов, указаний, инструкций) по эксплуатации ЗИС.
45. Оценка эффективности ЗИС: Проведение оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации. Критерии и показатели эффективности СЗИ ИС.
46. Оценка эффективности ЗИС: Разработка предложений по совершенствованию системы управления защиты информации автоматизированных систем. Принципы формирования политики информационной безопасности в автоматизированных системах

Образец экзаменационного билета:

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

10.04.01 Информационная безопасность

Дисциплина: Защищенные информационные системы

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 20

1. Методологии проектирования ИС. Этапы проектирования ИС.
2. ИС реального времени и требования к надежности таких ИС.

Зав. кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии оценки (в баллах):

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

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

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

- 0-10 баллов выставляется студенту, если он отказался от ответа или не смог ответить на вопросы билета, ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний.

Планы практических занятий

Раздел 1. Требования безопасности ЗИС

Практическое занятие 1. Представление о ЗИС (семинар) (2 часа)

Цель: знакомство с теоретическими представлениями об информационных процессах.

Содержание: Отчет на одну из тем из списка готовится каждым студентом в виде электронного текстового файла. Электронный вариант исследования с перечнем источников информации и ссылок на интернет-ресурсы или иные ресурсы следует прислать в почту как отчет к практике. Следует использовать информацию только из действующих нормативных документах (не использовать сведения из отмененных положений, ГОСТов, нормативов, приказов). Темы для проведения исследования (следует выбрать 1):

1. Информационные системы: содержание термина, определения ИС в ГОСТах, Приказах («Требованиях …», и др. нормативных документах) регуляторов в области ИБ.
2. Представление о защищенных ИС: определение, виды, требования к ЗИС, связанные с защищенностью).
3. Отличия ЗИС от ОИС. Области и специфика применения защищенных ИС (цели, задачи обеспечения ИБ объектов; области применения ЗИС (медицина, госуправление, правоохранительные органиы/МВД); примеры.
4. Классы информационных систем с точки зрения их функционала и видов обрабатываемой в них информации.
5. Проблемы информационной безопасности при использовании ИС, АИС, АСУ.
6. Виды и свойства информации. Угрозы информационной безопасности, реализуемые в отношении ИС.
7. Нормативно-законодательные положения/документы по защите информационной безопасности в защищенных информационных системах.
8. АИС, АС в защищенном исполнении – конкретные примеры с характеристиками, функциональности и описанием штатных средств безопасности.

Практическое занятие 2. Представление об информационной безопасности в ЗИС. Стандарты информационной безопасности для ИС/АС (2 часа)

Содержание: Отчет на одну из тем из списка готовится каждым студентом в виде электронного текстового файла. Электронный вариант исследования с перечнем источников информации и ссылок на интернет-ресурсы или иные ресурсы следует прислать в почту как отчет к практике. Следует использовать информацию только из действующих нормативных документах (не использовать сведения из отмененных положений, ГОСТов, нормативов, приказов). Вдвоем на одну тему готовить материалы нельзя.

Темы проведения исследования:

1. Международные стандарты, ГОСТы и нормативные документы, определяющие требования к защищенности ИС/АС.
2. Нормативная база, регламентирующая разработку и эксплуатацию ИАС.
3. Нормативные и методические документы регуляторов (ФСТЭК, ФСБ) - про ЗИС («Меры защиты информации в ГИС» и проч.) Уровни защищенности и классы ИС.
4. Угрозы ИБ, предпосылки уязвимости ИС.
5. Источники, способы и результаты дестабилизирующего воздействия на информацию; Их выявление и оценка (общий алгоритм и особенности).
6. Требования к уровню защищенности автоматизированных систем с учетом класса защищенности.
7. Методы и средства защиты информационных систем.
8. Проблема оценки защищенности информационных систем среды.

Практическое занятие № 3. Проблемы проектирования и разработки ЗИС (2 часа)

Содержание: Отчет на одну из тем из списка готовится каждым студентом в виде электронного текстового файла. Электронный вариант исследования с перечнем источников информации и ссылок на интернет-ресурсы или иные ресурсы следует прислать в почту как отчет к практике. Следует использовать информацию только из действующих нормативных документах (не использовать сведения из отмененных положений, ГОСТов, нормативов, приказов). Вдвоем на одну тему готовить материалы нельзя.

Темы проведения исследования:

1. Средства описания и моделирования деловых процессов, информационных процессов.
2. Действующие ГОСТы по разработке ИС/АС в защищенном исполнении и области применения подобных АС/ИС. Этапы разработки информационных систем
3. Уровни представления предметной области при проектировании информационной системы.
4. Составление задания на разработку ИС – методологические аспекты.
5. Проектирование ЗИС. Анализ и определение требований к уровню защищенности ПС/ИС
6. Программные закладки и методы противодействия.
7. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies.
8. Интеграция приложений и информационных систем.

Раздел 2. Представление о разработке информационных систем в защищенном исполнении

Практическое занятие 4. Теоретические основы построения защищённых автоматизированных систем (2 часа)

Цель: знакомство с теоретическими представлениями построения защищённых автоматизированных систем.

Содержание: Отчет на одну из тем из списка готовится каждым студентом в виде электронного текстового файла. Электронный вариант исследования с перечнем источников информации и ссылок на интернет-ресурсы или иные ресурсы следует прислать в почту как отчет к практике. Следует использовать информацию только из действующих нормативных документах (не использовать сведения из отмененных положений, ГОСТов, нормативов, приказов). Вдвоем на одну тему готовить материалы нельзя.

Краткий отчет результат исследования предлагается изложить в виде устного сообщения. Сделать это должен каждый студент группы во время практического занятия. Тему рекомендуется выбирать так, чтобы все темы списка оказались кем-либо из группы использованы.

Темы проведения исследования:

1. Основные термины и определения.
2. Техническое проектирование и реализация систем защиты.
3. Жизненный цикл системы.
4. Обзор подходов к созданию защищённых ИС (АС).
5. Проблемы проектирования и реализации защищенных АС. Проблемы интеграции.
6. Организационно-правовые аспекты защиты информации в АС.
7. Подходы к созданию защищённых систем.

Устный опрос по теме занятия (до 2 баллов за правильный ответ)

Практическое занятие № 5. Разработка и развёртывание защищённых ИС (2 часа)

Цель: знакомство с теоретическими представлениями построения защищённых автоматизированных систем.

Содержание: Отчет на одну из тем из списка готовится каждым студентом в виде электронного текстового файла. Электронный вариант исследования с перечнем источников информации

и ссылок на интернет-ресурсы или иные ресурсы следует прислать в почту как отчет к практике. Следует использовать информацию только из действующих нормативных документах (не использовать сведения из отмененных положений, ГОСТов, нормативов, приказов). Вдвоем на одну тему готовить материалы нельзя.

Краткий отчет результат исследования предлагается изложить в виде устного сообщения. Сделать это должен каждый студент группы во время практического занятия. Тему рекомендуется выбирать так, чтобы все темы списка оказались кем-либо из группы использованы.

1. Проблемы проектирования и реализации защищенных систем.
2. Методика определения состава защищаемой информации.
3. Этапы работы по выявлению состава защищаемой информации.
4. Требования к содержанию документов по общесистемным решениям.
5. Ведомость проекта. Пояснительная записка к проекту.
6. Роль специалиста по информационной безопасности в разработке, модернизации, внедрении ИС, в т.ч. защищенных ИС.
7. Стандарты проектирования систем защиты информации

Устный опрос по теме занятия (до 2 баллов за правильный ответ)

Практическое занятие № 6. Проектирование СЗИ для ИС (2 часа)

Цель: знакомство с теоретическими представлениями построения защищённых автоматизированных систем.

Содержание: Отчет на одну из тем из списка готовится каждым студентом в виде электронного текстового файла. Электронный вариант исследования с перечнем источников информации и ссылок на интернет-ресурсы или иные ресурсы следует прислать в почту как отчет к практике. Следует использовать информацию только из действующих нормативных документах (не использовать сведения из отмененных положений, ГОСТов, нормативов, приказов). Вдвоем на одну тему готовить материалы нельзя.

Краткий отчет результат исследования предлагается изложить в виде устного сообщения. Сделать это должен каждый студент группы во время практического занятия. Тему рекомендуется выбирать так, чтобы все темы списка оказались кем-либо из группы использованы.

1. Классификация угроз безопасности. Этапы создания модели угроз
2. Классификации уязвимостей системы
3. Модель нарушителя
4. Классификация нарушителей в соответствии с документами регуляторов.
5. Защита каналов утечки. Мониторинг (аудит) действий пользователей. Классификация внутренних нарушителей
6. Нетехнические меры защиты от внутренних угроз.
7. Криптографическая защита информации. Требования к шифрованию.
8. Требования к аутентификации в ИС. Аутентификация по IP-адресу.

Устный опрос по теме занятия (до 2 баллов за правильный ответ)

Практическое занятие № 7 Порядок аттестации автоматизированной системы (2 часа)

Цель: знакомство с теоретическими представлениями построения защищённых автоматизированных систем.

Содержание: Отчет на одну из тем из списка готовится каждым студентом в виде электронного текстового файла. Электронный вариант исследования с перечнем источников информации и ссылок на интернет-ресурсы или иные ресурсы следует прислать в почту как отчет к практике. Следует использовать информацию только из действующих нормативных документах (не использовать сведения из отмененных положений, ГОСТов, нормативов, приказов).

Краткий отчет результат исследования предлагается изложить в виде устного сообщения. Сделать это должен каждый студент группы во время практического занятия. Тему выбираете так, чтобы все темы списка оказались кем-либо из группы использованы.

1. Нормативная база организации работ по аттестации объектов информатизации (ОИ) по требованиям безопасности информации.
2. Назначение аттестации.
3. Схема организации и проведения работ по аттестации ОИ.
4. Функции организации-заявителя, ФСТЭК России и органов по аттестации ОИ.

Устный опрос по теме занятия (до 2 баллов за правильный ответ)

Практические занятия № 8, 9. Особенности построения систем защиты ИС (ЗИС) (2 часа)

Цель: знакомство с теоретическими представлениями построения защищённых автоматизированных систем.

Содержание: Отчет на одну из тем из списка готовится каждым студентом в виде электронного текстового файла. Электронный вариант исследования с перечнем источников информации и ссылок на интернет-ресурсы или иные ресурсы следует прислать в почту как отчет к практике. Следует использовать информацию только из действующих нормативных документах (не использовать сведения из отмененных положений, ГОСТов, нормативов, приказов). Вдвоем на одну тему готовить материалы нельзя.

Краткий отчет результат исследования предлагается изложить в виде устного сообщения. Сделать это должен каждый студент группы во время практического занятия. Тему выбираете так, чтобы все темы списка оказались кем-либо из группы использованы.

1. Особенности построения СЗИ для обработки ИСПДн
2. Нормативные документы. Угрозы для ИСПДн.
3. Особенности построения СЗИ для обработки ГИС
4. Нормативные документы. Угрозы для ГИС.
5. Лицензирование ПО.
6. Особенности построения СЗИ для обработки информации, содержащей коммерческую и служебную тайны.
7. Особенности построения СЗИ для обработки информации, содержащей государственную тайну.
8. Требование к оборудованию, ОС, применяемым для установки и использования ИС разных классов.

Тестирование (зачетное) до 20 баллов. Тест считается пройденным успешно при не менее 60% правильных ответов.

Критерии оценки результатов выполнения заданий практических занятий 1-2 разделов (в баллах*):*

- 4-5 баллов выставляется студенту, если работа практического занятия выполнена без ошибок и без замечаний (меньше баллов – 4 - выставляется, если есть мелкие замечания к качеству);
- 2-3 балла выставляется студенту, если работа выполнена с ошибками и/или поставленная в задаче цель достигнута частично (наполовину); такое же количество баллов (3) выставляется максимально за качественный устный доклад. За один семинар студент может выступить с докладом не более, чем по 2 темам.
- 1 балл выставляется студенту, если работа выполнена с ошибками и/или поставленная в задаче цель достигнута частично (менее, чем наполовину).

Раздел 3. Показатели качества и надежности ИС. Сертификация ИС

Практическое занятие № 10. Показатели качества и надежности ЗИС. Аудит защищённой ИС (2 часа)

Содержание: Устный опрос или письменный отчет минимум по 1 теме из списка тем для обсуждения ниже; выбор/формулировка темы КР, составление календарного плана работы над КР.

Темы для обсуждения, докладов, исследования:
1. Аудит информационной безопасности ИС.
2. Определение и классификации видов аудита.
3. Достоинства и недостатки видов аудита.
4. Назначение аудита. Последовательность действий в ходе аудита.
5. Методы аудита, мониторинга, выявления угроз ИБ
6. Возможности ЗИС. Средства безопасности, реализуемые в ЗИС.
7. Интерфейс ЗИС
8. Функциональные (встроенные) средства обеспечения безопасности ЗИС
9. Анализ уязвимостей с учетом модели нарушителя (инсайдера).
10. СЗИ конкретной ИС – обзор состава и администрирования /управления.
11. Аттестация ЗИС.

Устный опрос по теме занятий

2. Выбрать (или сформулировать) и сообщить тему курсового проекта на 1 практике (не позднее).

Темы для курсового проектирования по дисциплине Защищенные информационные системы (на 2 семестр 2021-2022 г.) для магистратуры 10.04.01 – Информационная безопасность:

1. Проектирование системы защиты информационной системы обработки информации, содержащей служебную тайну.
2. Проектирование системы защиты информационной системы обработки информации, содержащей коммерческую тайну.
3. Методология экономической оценки ущерба от угроз информационной безопасности для ИСПДн.
4. Методология оценки ущерба от угроз информационной безопасности для ИСОП.
5. Разработка подсистемы защиты данных информационной системы электронной библиотеки
6. Проектирование информационной системы в защищенном исполнении на конкретном примере системы электронного документооборота организации.
7. Проектирование информационной системы в защищенном исполнении на конкретном примере архива компании.
8. Проектирование информационной системы в защищенном исполнении на конкретном примере документационного хранилища организации).
9. Модернизация системы защиты информации в информационной системе (на конкретном примере) и экономическое обоснование затрат.
10. Разработка компонента безопасности для защищенной информационной системы (на конкретном примере).
11. Разработка частной модели угроз для системы защиты информации организации (на конкретном примере)
12. Проектирование системы защиты для инфраструктуры локальной сети (на конкретном примере).
13. Проектирование системы защиты для информационной корпоративной инфраструктуры, использующей внешнее облачное хранилища (на конкретном примере).

И др.

Примечание: Примеры конкретных ИС, для которых может быть выполнена разработка проекта ЗИС:

1. система управления производством;
2. система управления бизнес-процессами, информационным контентом организации (ECM, BPM);
3. система управления техническими средствами.
4. система маркетинга (CRM),
5. финансово-учетная система [банка, кредитной организации и т.п., где имеются специальные категории ПДн];
6. информационно-справочные и информационно-поисковые системы конкретных организаций [*коммерческих, бюджетных, органов управления муниципального/регионального уровня]*,
7. системы поддержки принятия решений и советующие системы,
8. Административная ГИС,
9. ИСПДн
10. Система обработки данных ЦОД или иного подобного оператора

Подробные методические пояснения см. в ФОС дисциплины.

Практическое занятие № 11-12. Моделирование угроз ИС по методике ФСТЭК
(4 часа)

Содержание: обследование объекта информатизации, оформление документации «Модель угроз информационной безопасности для [компонента] ИС».

Задача: Для выбранного по теме курсового проекта объекта информатизации (информационной системы или ее компонента) разработать модель угроз (рассматривайте эту работу как этап создания СЗИ ИС по теме своего курсового проекта: модель угроз должна послужить основой для составления технического задания на СЗИ ИС и частью проектной документации на СЗИ ИС). При оформлении документации «**Модель угроз** для [компонента] **информационной системы …** » используйте методику ФСТЭК моделирования угроз (вместо многоточия следует указать наименование конкретной программной или информационной системы, которая фигурирует в вашем курсовом проекте как объект исследования).

Оформленную документацию следует разместить в СДО в ДК «Защищенные информационные системы» по ссылке: https://sdo.bashedu.ru/mod/assign/view.php?id=66375 (Практика № 12-13)

Подробные методические пояснения см. в ФОС дисциплины.

Практическое занятие № 13. Разработка технического задания на СЗИ ИС (2 часа)

Содержание: по теме курсового проектирования для выбранной ИС/компонента ИС разработать техническое задание на создание/усовершенствование СЗИ ИС, с учетом выявленных актуальных угроз (согласно модели угроз, разработанной при выполнении практики 12-13).

Задание: Оформить техническое задание на СЗИ ИС (или СЗИ компонента ИС). ***Техническое задание на создание СЗИ ИС*** определяет:

- цель и задачи обеспечения защиты информации в ИС;
- требуемый класс защищенности ИС;
- перечень нормативных правовых актов, метод. документов и стандартов, которым должна соответствовать ИС и СЗИ ИС;
- перечень объектов защиты ИС;
- стадии (этапы работ) создания системы ЗИС;
- функции владельца/оператора ИС по обеспечению защиты ИС;

- обобщенные или детальные требования к техническим средствам, программному обеспечению, средствам защиты информации;
- требования к защите средств и систем, обеспечивающих функционирование информационной системы (обеспечивающей инфраструктуры);
- требования к защите информации при информационном взаимодействии с иными информационными системами и сетями.

Подробные методические пояснения см. в ФОС дисциплины.

Раздел 4. Внедрение и эксплуатация ЗИС

Практическое занятие № 14. Обзор ЗИС и технологий обеспечения безопасности работы ИС (примеры, характеристики ЗИС, области применения ЗИС, встроенные средства безопасности, возможности ЗИС) (2 часа)

Содержание: доклады или письменные исследования:
Темы для обсуждения/практической реализации/ исследования:

1. Основные направления защиты. Защита документов. Защита каналов утечки.
2. Мониторинг (аудит) действий пользователей.
3. Технические и программные средства аудита/контроля. Классификация внутренних нарушителей.
4. Сетевые фильтры – назначение, виды. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Технологии firewall. Политика безопасности firewall'a.
5. Системы анализа и оценки уязвимостей. Процесс анализа уязвимостей. Классификация инструментальных средств анализа уязвимостей. Возможности и недостатки систем анализа уязвимостей.
6. Цели и задачи использования IDS. Возможности IDS. Стратегия развертывания IDS. Типы атак, определяемых IDS.
7. Безопасность DNS. Сервисы DNS. Инфраструктура DNS. Компоненты DNS и понятие безопасности для них. Основные механизмы безопасности для сервисов DNS. Данные DNS и ПО DNS. Зонный файл. Name-серверы. Авторитетные name-серверы. Кэширующие name-серверы. Транзакции DNS. Запрос / ответ DNS.
8. Безопасность окружения DNS. Угрозы и обеспечение защиты платформы хоста. Угрозы ПО DNS. Угрозы для данных DNS.
9. Управление ресурсами на уровне ОС. Альтернативные платформы для web-сервера. Trusted ОС. Тестирование безопасности операционной системы. Действия для обеспечения безопасности ОС, на которой выполняется web-сервер.
9. Уязвимости технологий активного содержимого на стороне клиента. Уязвимости технологий создания содержимого на стороне сервера. Список действий для обеспечения безопасности web-содержимого.
10. Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе.

Подробные методические пояснения см. в ФОС дисциплины.

Практическое занятие № 15. Администрирование и эксплуатация защищенной ИС/АС. Управление рисками и инцидентами управления безопасностью (2 часа)

Содержание: задания для исследования, доклады; практические задания.

Теоретическая часть (1,5 часа)
1. Средства обеспечения отказоустойчивости автоматизированной системы
2. Порядок выполнения обязанностей администратора автоматизированной системы
3. Эксплуатационная документация защищенной автоматизированной системы
4. Нетехнические меры защиты от внутренних угроз.

5. Технологии и средства обеспечения защиты инфраструктуры от сетевых угроз (защита эл.почты, веб-приложений, доменных имён, информационных ресурсов, доступных из сети Интернет, обеспечение безопасности при удаленной работе сотрудников/пользователей с ИС и т.д.).

Практическая часть (0,5 часа)

а) Базовые элементы и устройства обеспечения сетевой безопасности ИС. Компоненты инфраструктуры ИС.

б) Практика использования конкретной ИС/ЗИС. Знакомство с интерфейсом ИС/ЗИС, функционалом, встроенными средствами безопасности и т.д.

Подробные методические пояснения см. в ФОС дисциплины.

Практическое занятие № 16 (2 часа)

Содержание занятия:

Вводная: с учетом новых угроз ИБ, создавшихся для РФ в условиях проведения СВО, НКЦКИ[1] недавно издал рекомендации субъектам КИИ РФ (и другим учреждениям, организациям, компаниям, информ. объектов РФ) по совершенствованию защиты их информационной инфраструктуры. (Текст этих рекомендаций см. в метод. указаниях).

Задание:

1) На основе бюллетеня НКЦКИ (Национальный координационный центр по компьютерным инцидентам) от 29.03.2022 «Обобщенные рекомендации по минимизации возможных угроз информационной безопасности информационным ресурсам РФ» попробуйте составить адаптированный опросный лист (анкету) для проведения самообследования ИБ-специалистами организации ее информационной системы, на предмет выполнения рекомендаций.

Примечание: На практике каждая организация может выборочно применить те из рекомендованных НКЦКИ мер защиты, которые актуальные для ее информационной инфраструктуры. Конкретный пример сокращенного перечня рекомендаций для учебных учреждений: http://uuonyurba.ru/wp-content/uploads/2022/04/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F-%D0%B7%D0%B0%D1%89%D0%B8%D1%89%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%8C.pdf

2) Проведите с использованием этой своей анкеты обследование уровня защищенности той ИС, которая является объектом защиты вашего курсового проекта. Результаты анкетирования изложите (со своими ответами типа «выполнено» - или почему та или иная рекомендация не может быть на данный момент выполнена).

Подробные методические пояснения см. в ФОС дисциплины.

Практическое занятие № 17. Технические средства защиты информации в ИС (2 часа)

Содержание: (задания для исследования, доклады, тематика выполнения задания)

1. Актуальные проблемы и риски защищенности ресурсов и данных в ИС.

[1] Полномочия НКЦКИ (созданного в 2018 г. приказом ФСБ): обеспечивает координацию деятельности субъектов КИИ РФ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Функции НКЦКИ: координация мероприятий по реагированию на компьютерные инциденты; обнаружение, предупреждение и ликвидация последствий компьютерных атак; доведение до субъектов КИИ информации о методах предупреждения и обнаружения компьютерных атак. См. подробности здесь, например: https://www.tadviser.ru/a/425856 или в приказе ФСБ.

2. Технические средства защиты информации в ИС.
3. Обеспечение совместимости ИС и технических средств защиты.
4. Выполнение классификации внутренних нарушителей (для конкретной ИС).
5. Классификация инструментальных средств анализа уязвимостей.
6. IDS-системы. Типы компьютерных атак, определяемые IDS.
7. Аутентификация, основанная на IP-адресе.
8. Сканирование уязвимостей (средства).
9. Тестирование проникновения (средства).
10. Развертывание интерактивных детекторов атак на виртуально-физической инфраструктуре.

Тест компьютерный.

Критерии оценки результатов выполнения заданий лабораторных занятий 3-4 разделов (в баллах*):*

- 3-4 балла выставляется студенту, если работа практического занятия выполнена без ошибок и без замечаний (меньше баллов – 3 - выставляется, если есть мелкие замечания к качеству);
- 2 баллов выставляется студенту, если работа выполнена с ошибками и/или поставленная в задаче цель достигнута частично (наполовину); такое же количество балов выставляется максимально за качественный устный доклад. За один семинар студент может выступить с докладом не более, чем по 2 темам.
- 1 балл выставляется студенту, если работа выполнена с ошибками и/или поставленная в задаче цель достигнута частично (менее, чем наполовину).

Лабораторные задания

Раздел 1. Требования безопасности ЗИС

Лабораторное занятие 1. Требования к проектной документации по ЗИС (4 часа)

Содержание:

1. Ознакомится с ГОСТами на разработку технического задания по созданию системы защиты для ИС (*или ИС в защищенном исполнении, - на выбор студента*).
2. Ознакомиться со стандартами и требованиями по обеспечению защиты ИС (конкретные варианты задания - для конкретных классов ИС/АС); включить в техническое задание те требования, которые соответствуют классу/виду компонентов предполагаемой ИС – объекта защиты. В качестве защищаемой ИС студенту предлагается взять систему электронного документооборота (например, DeirectumRX с локальным хранилищем документов или документационным хранилищем на сервере вендора программы в г. Ижевск) небольшой коммерческой компании, предоставляющей услуги проектирования частных домов для населения. Виды документации, число и категории сотрудников, а также виды защищаемых информационных ресурсов продумайте самостоятельно. Организация расположена в Уфе, занимает арендуемые помещения в здании бизнес-центра (где арендуют помещения и другие организации), на входе в центр имеется СКУД https://www.parsec.ru/products/parsecnet3/; в помещения находятся рабочие места (настольные и переносные компьютеры, соединенные локальной радиосетью, оснащенные Windows 10, антивирусом Kaspersky EDR…).
3. Оформить часть проектной документации - **техническое задание** - на проектирование указанной СЗИ ИС в соответствии со стандартами и требованиями к СЗИ ИС (ссылки и теоретические материалы см. в лекциях в дистанционном курсе ЗИС https://sdo.bashedu.ru/course/view.php?id=1467

Подробные методические пояснения см. в ФОС дисциплины.

Критерии оценки: до 10 баллов, с учетом полноты и правильности оформления документации по заданиям.

Раздел 2. Представление о разработке информационных систем в защищенном исполнении

Лабораторное занятие № 2. Обследование предметной области, моделирование угроз при проектировании ЗИС (6 часов)

Содержание:

- Изучить стандарты по созданию технического проекта ЗИС, методические документы по моделированию угроз ИБ при проектировании ЗИС.
- Обследовать (продумать) выбор инструментов описания/моделирования схем и процессов (для описания рабочих процессов обработки конфиденциальных документов в ИС (в т.ч. СЭД)). Разработать модели рабочих процессов по обработке КД с ИС, матрицы объектом и субъектов доступа к защищаемым ресурсам, с указанием уровней доступа разных категорий персонала (ролей пользователей) – как есть (as is). Это позволит оценить на следующем шаге угрозы и уязвимости ИБ.

  Стандартные встроенные средства обеспечения информационной безопасности и защиты информации в типичной СЭД:

  1. Аутентификация пользователя системы (метод аутентификации и количество уровней аутентификации различны).
  2. Распределение прав доступа для пользователей системы.
  3. Поддержка электронной подписи (в т.ч. встроенная в СЭД).
  4. Шифрование при хранении и передаче электронных документов.
  5. Протоколирование и аудит работы пользователей в системе.

- Разработать модель угроз и модель нарушителя; оценить ценность/стоимость защищаемых ресурсов (в выбранной шкале оценки); составить перечень актуальных угроз (не более 3, например, по одной угрозе каждого вида); продумать и описать сценарии реализации актуальных угроз. Ранжировать угрозы по величине риска.

  Примечание: Среди угроз для систем электронного документооборота можно выделить следующие виды:

  1. Угрозы целостности – повреждение, искажение или уничтожение информации (случайное, преднамеренное).
  2. Угрозы конфиденциальности – кража информации, подмена маршрутов обработки, перехват, несанкционированный доступ к информации.
  3. Угрозы доступности (нормальному функционированию системы): ошибки пользователей, внешние сетевые атаки, вредоносное ПО, сбои в работе оборудования и программном обеспечения.

  Пример перечня угроз для СЭД приведен в приложении.
- С учетом проделанного анализа сформулировать требования по безопасности. Разработать профили разграничения прав доступа к информационным ресурсам, в зависимости от структурной и/или должностной принадлежности сотрудников.
- Промежуточные результаты анализа и выводы оформить в виде технического проекта на создание СЗИ.

Разработанную документацию следует разместить для проверки в ДК ЗИС по ссылке: https://sdo.bashedu.ru/mod/assign/view.php?id=56657

Подробные методические пояснения см. в ФОС дисциплины.

Лабораторное занятие №. 3. Теоретические основы построения защищённых автоматизированных систем (4 часа)

Содержание:

- Дать характеристику подходам к созданию защищённых ИС (АС).
- Описать этапы проектирования и реализации защищенных АС.
- Привести перечень актуальных стандартов и нормативных документов, которые требуется учитывать при разработке АСЗИ.
- Составить с учетом проекта СЗИ перечень мер защиты от актуальных угроз. Оценить временные, финансовые затраты на реализацию предлагаемого проекта внедрения и эксплуатации СЗИ на 1 год (или 3 года).

Подробные методические пояснения см. в ФОС дисциплины.

Лабораторное занятие № 4. Разработка и развёртывание защищённых ИС (4 часа)

Содержание: Оценка эффективности проекта ЗИС:

- описать порядок проведения исследования,
- методы и методики, средства для проведения анализа эффективности ЗИС,
- документальное оформление результатов оценки (применительно к проекту СЗИ, который разрабатывался в течение 3-х предшествующих лабораторных работ). При оформлении проектной документации и выполнении расчетов следовать рекомендациям ГОСТ и метод.документов регуляторов в области ИБ

Подробные методические пояснения см. в ФОС дисциплины.

Критерии оценки за выполнение каждой из 4-х лабораторных заданий 1-го семестра (1-2 разделы курса): до 10 баллов, с учетом полноты и правильности оформления документации по заданиям.

Разделы 3, 4.

Лабораторное занятие № 5. Инструментальное обследование уровня защищенности ИС (4 **часа)**

Содержание: Инструментальное обследование уровня защищенности конкретной ИС. Методические разъяснения приводятся во время занятия.

Альтернативное лабораторное занятие № 5. Защищенные системы. Инструментальное обследование уровня защищенности ИС (4 часа)

1. *Изменение политики безопасности в условиях санкционных ограничений на ПО.*
2. *Подбор защищенных компонентов для ИС (варианты ЗИС: для защиты коммерческой тайны, для защиты ПДн, для защиты служебной тайны)*
3. *Инструментальное обследование уровня защищенности конкретной ИС*

1. Проанализировать новые условия, в которых оказалась информационная инфраструктура РФ и обозначить риски, новые угрозы, найти документы регуляторов и органов власти, направленные на противодействие этим угрозам в сфере IT. Сделать обзор, привести ссылки. сделать резюме по результату решения задачи. – см. вводную часть ниже.

2. Подбор защищенных компонентов для ИС**.** Выбрать вид информации, обработку которую в условиях санкционных рисков требуется обеспечивать гипотетической организации/структуре (ПДн, коммерческая тайна, служебка, личное рабочее место и проч.). Определить, с учетом вида информации и новых (санкционных и военных) рисков, обобщенный перечень угроз. С учетом угроз, подобрать комплекс компонентов ИС (компьютеров, сетевого оборудования, системного и прикладного ПО), способный обеспечить устойчивое выполнение рабочих задач и защиту информации (или, шире, рабочей среды) от угроз ИБ. Для указанных компонентов ИС следует привести характеристики, подтверждающие способность системы обеспечить защищенную работу.

Например, если стоит задача обеспечить мобильную корпоративную среду с высоким уровнем защищенности, с учетом требования использовать только или преимущественно отечественное «железо» и ПО[2], можно посмотреть в сторону российских мобильных устройств, укомплектованных российским сертифицированным (в т.ч. защищенным) ПО, ОС и проч.)

Подробные методические пояснения см. в ФОС дисциплины.

Лабораторное занятия № 6. Особенности построения систем защиты ИС (ЗИС) (6 часов)

Содержание:
Задание 1. (4 часа)
Инструментальное обследование уровня защищенности конкретной ИС (выбранной объектом исследования в рамках курсового проекта), используя доступные документы и иные сведения о политике безопасности в исследуемой ИС, настройки параметров безопасности компонентов ИС, возможно, инструменты для пен-тестинга и методы OSINT, оценить уровень уязвимости данных ИС по отношению к различным угрозам информационной безопасности (перечень угроз должен определяться в ходе **выполнения практического задания 12-13** (https://sdo.bashedu.ru/mod/assign/view.php?id=66375)).

Задание 2 (на выбор) (2 часа)
1) Сформулировать особенности и порядок построения СЗИ для обработки ИСПДн
2) Сформулировать особенности и порядок построения СЗИ для обработки ГИС
3) Сформулировать особенности и порядок создания СЗИ для обработки информации, содержащей коммерческую тайну.
4) Сформулировать особенности и порядок построения СЗИ для обработки информации, содержащей государственную тайну.
5) Требование к оборудованию, ОС, применяемым для установки и использования ИС разных классов.

Подробные методические пояснения см. в ФОС дисциплины.

Лабораторное занятие 7. Разработка проектных документов для ЗИС. Оценка эффективности ЗИС (8 часов)

Содержание: Описать, какие сведения необходимы для составления задания на разработку ЗИС, для проектирования ЗИС. Разработать техническое задание на разработку ЗИС по заданию (для конкретной ИС).

- Разработка документов по обследованию ИС и проектированию ЗИС.
- С учетом требований нормативных и методическим документов (в т.ч. методики ФСТЭК от 5 февраля 2021 г. «Методика оценки угроз безопасности информации») произвести обследование ИС, построить модель угроз и нарушителя, определить класс защищенности ИС, сформулировать требования по обеспечению ИС средствами защиты информации (с подробной характеристикой средств ЗИ по классу защиты и уровню доверия, отвечающих классу защищенности ИС).
- Выполнить примерную экономическую оценку затрат на программно-технические меры защиты (или описать подробный алгоритм такой оценки)

---

[2] Владельцам объектов КИИ, согласно Указу Президента РФ от 07 мая 2018 г. № 204, необходимо было перейти на преимущественное использование российского ПО до 01.01.2021, перейти на преимущественное использование российского
оборудования до 01.01.2022, с 2021 г использовать в отечественных системах хранения документов только системы хранения
с отечественными микропроцессорами.

- Сформулировать организационные мероприятия по защите информации в ЗИС.
- Политику безопасности в отношении указанной ИС оформить в соответствии с принятыми требованиями и стандартами.
- Описать процедуры развертывания СЗИ ИС.
- Оценка эффективности ЗИС.

Подробные методические пояснения см. в ФОС дисциплины.

Критерии оценки за выполнение каждой из лабораторных заданий 2-го семестра (3-4 разделы курса): до 10 баллов, с учетом полноты и правильности оформления документации по заданиям.

Типовые тестовые задания

При изучении дисциплины используются тестовые задания закрытого и открытого типа. Каждое тестовое задание включает вопрос и несколько вариантов ответов к нему. Необходимо выбрать один ответ из предложенных вариантов (если в задании не указано иное).

Тестирование выполняется в виде компьютерного тестирования в СДО и личном кабинете студента (2 теста - по результатам 1 и 2 семестров).

Примеры тестовых вопросов:

1. Что описывают/регламентируют ГОСТ Р 56939-2016 и ГОСТ Р 58412-2019 ? (выберите наиболее правильную характеристику):
- стадии разработки безопасного программного обеспечения и меры защиты от угроз ИБ на этапах разработки
- требования к уровню защищенности информационных системы
- разработку системы защиты информации для ИС
- порядок создания автоматизированных систем в защищенном исполнении

2. Под информационной системой понимается прикладная программная подсистема, ориентированная на сбор, хранение, поиск и _____текстовой и/или фактографической информации ***(вставьте правильное слово винительном падеже)***
обработку

3. Деление информационных систем на одиночные, групповые, корпоративные, называется классификацией… ***(выберите правильное)***
По масштабу;
По сфере применения;
По способу организации;
По уровню безопасности

4. Что описывает/регламентирует ГОСТ Р 51583-2014? ***(выберите наиболее правильную характеристику):***
- порядок создания автоматизированных систем в защищенном исполнении
- стадии разработки программного обеспечения
- требования к уровню защищенности информационных системы
- разработку системы защиты информации для ИС

5. Как понимается термин «АВТОМАТИЗИРОВАННАЯ СИСТЕМА» по ГОСТ 34.003 ? **«АС – это …» (*продолжите определение, выбрав правильное из ниже предложенного):***
- это система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

- это организационно упорядоченная совокупность программно-аппаратных и других вспомогательных средств, обеспечивающая возможность надежного долговременного хранения больших объемов информации, поиска и обработки данных в соответствии с требованиями предметной области, а также поддерживающая удобный интерфейс с пользователями системы. Включает компьютерное и коммуникационное оборудование, программное обеспечение, информационные ресурсы;
- это совокупность компонентов, коммуникаций, контента, образующих отграниченную от окружающей среды целостность, выполняющая функцию обработки, хранения и трансляции информации;
- это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

… и т.д. (подробнее см. ФОС дисциплины)

Тестирование №1 проходит в личном кабинете учащегося (ссылка на тест «Защищенные информационные системы: Тест ЗИС №1 (за 1 семестр)» - https://cabinet.bashedu.ru)

Критерии оценки результатов тестирований (в баллах)*:*

-0,83 балла в тесте 1 выставляется студенту за каждый тестовый вопрос, если ответ на вопрос теста дан верно;
-0 баллов выставляется студенту за каждый тестовый вопрос, если ответ на вопрос теста дан ошибочный;

Тест № 1 по результату освоения разделов (модулей) 1 семестра состоит из 24 вопросов и оценивается в совокупности до 20 баллов (Тест проводится в личном кабинете студента. Ссылка на тест: https://cabinet.bashedu.ru/tests/dev/quiz/view/2299).

Возможно итоговое тестирование № 2 по результату освоения разделов 3,4 (2 семестр) (до 10 тестовых вопросов (по 0,5 балла за тестовый вопрос), в совокупности до 5 баллов за тестирование.

Темы для курсового проектирования
по дисциплине **Защищенные информационные системы (на 2 семестр 2021-2022 г.)**
Для магистратуры 10.04.01 – Информационная безопасность

1. Проектирование системы защиты информационной системы обработки информации, содержащей служебную тайну.
2. Проектирование системы защиты информационной системы обработки информации, содержащей коммерческую тайну.
3. Методология экономической оценки ущерба от угроз информационной безопасности для ИСПДн.
4. Методология оценки ущерба от угроз информационной безопасности для ИСОП.
5. Разработка подсистемы защиты данных информационной системы электронной библиотеки
6. Проектирование информационной системы в защищенном исполнении на **конкретном примере** системы электронного документооборота организации.
7. Проектирование информационной системы в защищенном исполнении на конкретном примере архива компании.
8. Проектирование информационной системы в защищенном исполнении на **конкретном примере** документационного хранилища организации).
9. Модернизация системы защиты информации в информационной системе (на **конкретном примере**) и экономическое обоснование затрат.

10. Разработка компонента безопасности для защищенной информационной системы (на **конкретном примере**).
11. Разработка частной модели угроз для системы защиты информации организации (на **конкретном примере**)
12. Проектирование системы защиты для инфраструктуры локальной сети (на **конкретном примере**).
13. Проектирование системы защиты для информационной корпоративной инфраструктуры, использующей внешнее облачное хранилища (на **конкретном примере**).

Примечание: Примеры конкретных ИС, для которых может быть выполнена разработка проекта ЗИС:

- системы управления производством;
- системы управления бизнес-процессами, информационным контентом организации (ECM, BPM);
- системы управления техническими средствами.
- системы маркетинга (CRM, BI),
- финансовые и учетные ИС/АС;
- информационно-справочные и информационно-поисковые системы,
- системы поддержки принятия решений и советующие системы,
- государственные административные ГИС,
- ИСПДн

…

Методические пояснения приведены в ФОС и методических рекомендациях по курсовому проектированию

Критерии оценки:

- ***«отлично»*** ***(*****12-15 баллов)** – курсовая работа (проект) выполнена в полном объеме, оформлена по ГОСТам и требованиям (см. методические рекомендации по написанию курсовых проектов), в рекомендуемой логической последовательности, с точным использованием специализированной терминологии; цель и задачи, поставленные студентом, достигнуты, при этом показано уверенное владение теоретическими и практическими компетенциями. Разъяснения в процессе презентации результатов курсового проектирования (защиты КП) - исчерпывающи, отражают полноту и правильность усвоения студентом материалов дисциплины и достигнутых в ходе проектирования результатов. Студент свободно ориентируется в теме, дает правильные и полные ответы на вопросы по теме курсового проекта.
- ***«хорошо»*** ***(*****8-11 баллов) -** курсовая работа (проект) выполнена в полном объеме, оформлена по ГОСТам и требованиям (см. методические рекомендации по написанию курсовых проектов), в рекомендуемой логической последовательности, с точным использованием специализированной терминологии; цель и задачи, поставленные студентом, в-целом, достигнуты, при этом показано хорошее е владение теоретическими и практическими компетенциями. Однако отчет оформлен с мелкими нарушениями или имеются незначительные неточности или пробелы при оформлении документации;
- ***«удовлетворительно»*** ***(*****4-7 балла)** - курсовая работа (проект) выполнена частично объеме, оформлена по ГОСТам и требованиям (см. методические рекомендации по написанию курсовых проектов) с небольшими ошибками, но в рекомендуемой логической последовательности, с правильным использованием специализированной терминологии; цель и задачи, поставленные студентом, достигнуты не менее чем на 50%, при этом показано удовлетворительное владение теоретическими и практическими компетенциями. Однако отчет оформлен с нарушениями или имеются незначительные неточности или пробелы при оформлении документации; (неполнота отчета наблюдается в части документов приложения или оформления текста, либо экономическое обоснование проекта сделано с ошибками или частично, либо плохо обосновано по иным причинам), либо не показано четкое

понимание студентом материала темы, выявлена недостаточная сформированность некоторых основных умений и навыков.

- ***«неудовлетворительно»*** **(1-3 балла)** - выставляется, если лабораторная работа выполнена с грубыми нарушениями требований к оформлению и содержанию, документация оформлена неверно и нерационально, с грубыми нарушениями требований ГОСТов и метод. документов регуляторов. Поставленные цели и задачи не достигнуты.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. Шкундин С.З., Берикашвили В.Ш.Теория информационных процессов и систем: учебное пособие. - М.: Горная книга, 2012. – 475 с. http://biblioclub.ru/index.php?page=book&id=229031&sr=1
2. Громов Ю.Ю., Дидрих В.Е., Иванова О.Г., Однолько В.Г.Теория информационных процессов и систем: учебное пособие. - Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2014. – 172 с. - http://biblioclub.ru/index.php?page=book&id=277939&sr=1
3. Душин В.К.Теоретические основы информационных процессов и систем: учебник. - М.: Дашков и Ко, 2014. – 348 с. - http://biblioclub.ru/index.php?page=book&id=221284&sr=1

Дополнительная литература:

4. Аверченков В.И., Лозбинев Ф.Ю., Тищенко А.А.Информационные системы в производстве и экономике: учебное пособие. - М.: Флинта, 2011. – 274 с. - http://biblioclub.ru/index.php?page=book&id=93265&sr=1
5. Алдохина О.И., Басалаева О.Г.Информационно-аналитические системы и сети: учебное пособие, Ч. 1. Информационно-аналитические системы: Учебное пособие. - Кемерово: КемГУКИ, 2010. – 148 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=227684&sr=1
6. Блинков Ю.В. Основы теории информационных процессов и систем: учебное пособие. - Пенза. Пензенский государственный университет архитектуры и строительства. – 2011, 184 с. – Режим доступа: http://window.edu.ru/resource/055/78055/files/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D1%8B_%D1%82%D0%B5%D0%BE%D1%80%D0%B8%D0%B8_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%BE%D0%B2.pdf
7. Бураков П.В., Петров В.Ю. Информационные системы в экономике: Учебное пособие. - СПб.: СПбГУ ИТМО, 2010. - 66 с. - http://window.edu.ru/resource/399/67399/files/itmo436.pdf
8. Бурцева Е.В., Рак И.П., Селезнев А.В., Терехов А.В., Чернышов В.Н. Информационные системы: Учебное пособие. - Тамбов: Изд-во ТГТУ, 2009. - 128 с. - http://window.edu.ru/resource/260/68260/files/Terehov_c.pdf
9. Володин Д.О., Матчин В.Т., Минаков В.И., Мордвинов В.А., Романов Д.Д., Третьяков А.А., Шленов А.Ю. и др. Моделирование информационных процессов и систем. - М.: МГДД(Ю)Т, МИРЭА, ГНИИ ИТТ "Информика", 2002. - 50 с. - http://window.edu.ru/resource/015/47015/files/mirea015.pdf
10. Гарифуллина С.Р. Система управления базами данных: Учебное пособие для студентов и магистрантов естественнонаучных и гуманитарных факультетов университета..

– Уфа: РИЦБашГУ, 2012. – 80 с. - https://bashedu.bibliotech.ru/Reader/Book/2013051610235800379600002120
11. Гвоздева В.А. Информатика, автоматизированные информационные технологии и системы: учебник / – М.: ИД «ФОРУМ»: ИНФРА-М, 2011. – 544с
12. Горбаченко В. И. и др. Проектирование информационных систем с CA ERwin Modeling Suite 7.3: учебное пособие / В. И. Горбаченко, Г. Ф. Убиенных, Г. В. Бобрышева – Пенза: Изд-во ПГУ, 2012. – 154 с.2.
13. Громов Ю.Ю.,ИвановаО.Г.,СерегинМ.Ю.,Ивановский М.А.,ДидрихВ.Е.Архитектура ЭВМ и систем: Учебное пособие для студентов высших учебных заведений. – Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2012. – 200 с. - http://biblioclub.ru/index.php?page=book&id=277352
14. Гуде С.В., Ревин С.Б. Информационные системы: Учебное пособие. - Ростов-на-Дону: Ростовский юридический институт МВД России, 2002. - 149 с. - http://window.edu.ru/resource/483/57483/files/infsist.pdf
15. Д. В. Александров. Инструментальные средства информационного менеджмента. CASE-технологии и распределенные информационные системы: учебное пособие. М.: Финансы и статистика. 2011 – 225 с. ЭБС «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=85069
16. Ковальчук С.В., Лямин А.В. Информатика. Информационно-управляющие системы. Учебно-методическое пособие. - СПб.: СПбГУ ИТМО, 2003. - 28 с. - http://window.edu.ru/resource/016/24016/files/project.pdf
17. Максимов Н.В., Голицына О.Л., Тихомиров Г.В., Храмцов П.Б.Информационные ресурсы и поисковые системы: учебное пособие. - М.: МИФИ, 2008. – 400 с. - http://biblioclub.ru/index.php?page=book&id=231125&sr=1
18. Матвейкин В.Г., Дмитриевский Б.С., Ляпин Н.Р. Информационные системы интеллектуального анализа. - М.: Машиностроение, 2008. - 92 с. - http://window.edu.ru/resource/097/64097/files/lapin-a.pdf
19. Нестеров С.А. Информационная безопасность и защита информации: Учебное пособие. - СПб.: Изд-во Политехн. ун-та, 2009. - 126 с. - http://window.edu.ru/resource/462/67462/files/%D0%BF%D0%BE%D1%81%D0%BE%D0%B1%D0%B8%D0%B5%D0%98%D0%91%D0%97%D0%98.pdf
20. Федотова Е. Л. Информационные технологии и системы: Учебное пособие - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 352 с. ISBN 978-5-8199- 0376-6 / ЭБС «Знаниум» http://znanium.com/bookread2.php?book=429113
21. Электронный учебник "Информационные процессы" (Омск, 2001) - http://www.univer.omsk.su/omsk/Edu/infpro/infpro.html

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

- Словари и энциклопедии On-Line- http://www.dic.academic.ru
- Электронная библиотечная система БашГУ – www.bashlib.ru
- Электронная библиотечная система «ЭББашГУ» - https://elib.bashedu.ru/
- Электронная библиотечная система «Университетская библиотека онлайн» - https://biblioclub.ru/
- Электронная библиотечная система издательства «Лань» - https://e.lanbook.com/
- Электронный каталог Библиотеки БашГУ - http://www.bashlib.ru/catalogi/
- Справочная правовая система «КонсультантПлюс» - http://www.consultant-plus.ru
- Журнал Научно-техническая информация. Серия 2. Информационные процессы и системы (по годам)

Программное обеспечение

1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.
4. 1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях. Договор № 1199 от 09.01.2019 г.
5. Система DirectumRX (ежегодно пролонгируемый договор с компанией Directum (Ижевск) о предоставлении бесплатного учебного доступа к облачной платформе).

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 № 516. 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/1	Лекции	Аудитория № 516. Оборудование: учебная мебель, доска, кресла секционные последующих рядов с пюпитром, проектор Epson eb-535w, экран на штативе Eco Picture(200x127), моноблок 23,6" Powercool
2. Учебная аудитория для проведения занятий семинарского типа: Аудитория № 508. Аудитория № 509. Лаборатория моделирования процессов защиты информации. Аудитория № 404. Специализированный кабинет с лабораторным оборудованием. 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/1	Практические и лабораторные занятия	Аудитория № 508. Специализированная аудитория с лабораторным оборудованием. Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, учебно-демонстрационная панель «Монтаж средств технической защиты информации. Аудитория № 509. Лаборатория моделирования процессов защиты информации. Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, учебно-лабораторный стенд «Сетевая безопасность». Аудитория № 404. Специализированный кабинет с лабораторным оборудованием. Оборудование: учебная мебель, системные блоки\i5-10400 (2.9GHz)\H510M\8Gb\HDD 1Tb\корпус Micro ATX\Win10 Pro, мониторы ЖК 23.8" LG 24MK430H-B (1920x1080, IPS,75 Гц, 5 мс, 1000:1, 250 кд/м2, D-Sub, HDMI, кабель HDMI в комплекте), виртуальный тренажер «Аттестация объекта по требованиям защиты от утечек информации по техническим каналам».
3. Учебная аудитория для проведения групповых и индивидуальных консультаций: Аудитория № 608 450076, Республика Баш-	консультации	Аудитория № 608 Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, телевизор TCL-L55P6US.

кортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/1		
4. Учебная аудитория для текущего контроля и промежуточной аттестации: Аудитория № 404. Специализированный кабинет с лабораторным оборудованием. 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/1	**текущий контроль и промежуточная аттестация**	Аудитория № 404. Специализированный кабинет с лабораторным оборудованием. Оборудование: учебная мебель, системные блоки\i5-10400 (2.9GHz)\H510M\8Gb\HDD 1Tb\корпус Micro ATX\Win10 Pro, мониторы ЖК 23.8" LG 24MK430H-B (1920x1080, IPS,75 Гц, 5 мс, 1000:1, 250 кд/м2, D-Sub, HDMI, кабель HDMI в комплекте), виртуальный тренажер «Аттестация объекта по требованиям защиты от утечек информации по техническим каналам».

Приложение № 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Защищенные информационные системы
на _1_ семестр
очная форма обучения

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (з.е. / часов)	3/72
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
из них, предусмотренные на выполнение курсовой работы / курсового проекта	
Учебных часов на самостоятельную работу обучающихся (СР)	17,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	
Учебных часов на подготовку к экзамену	0

Форма контроля:
Зачет 1 семестр

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины «Защищенные информационные системы»
на 2 семестр
очная форма обучения

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (з.е. / часов)	3/108
Учебных часов на контактную работу с преподавателем:	51,2
лекций	16
практических/ семинарских	16
лабораторных	
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	3,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	2
Учебных часов на самостоятельную работу обучающихся (СР)	29,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	17
Учебных часов на подготовку к экзамену (Контроль)	27

Формы контроля:
Курсовое проектирование 2 семестр
Экзамен 2 семестр

№ п/п	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				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
Раздел 1. Требования безопасности ЗИС							
1.	1.1. Виды и категории программных систем. Категории ИС с повышенными требованиями к защищенности **Содержание:** Открытые и защищенные ИС. Средства защиты открытых информационных систем. Виды и примеры защищенных ИС. Концепция «защищенные информационные системы»	2	2	2	2	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;
2.	1.2. Международные стандарты, ГОСТы и нормативные документы, определяющие требования к защите ИС/АС. Уровни защищенности и классы ИС. Требования к уровню защищенности автоматизированных систем с учетом класса защищенности. Угрозы и уязвимости ИС **Содержание**: отечественные стандарты защищенности – о требованиях к ИС. Требования к защищенности ИС с учетом обрабатываемой в них информации, масштаба, функционального назначения и т.д. Нормативные и методические документы регуляторов (ФСТЭК, ФСБ) про ЗИС.	2	2		2	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;

	Уровни защищенности и классы ИС						
3	1.3. Требования международных, национальных и отраслевых стандартов к разработке и обеспечению безопасности защищенных ИС **Содержание**: Фрагментарный и комплексный и подходы к защите ИС; эшелонированная защита. Требования к уровню защищенности ИС/АС с учетом класса защищенности. Классификации ИС по требованиям к уровню защищенности обрабатываемых в них данных. Определение уровня защищенности персональных данных для ИСПДн; классы защищенности ГИС; классы ИСОП; классы защищенности автоматизированной системы управления (в т.ч. АСУТП); категории значимости ИС, отнесенных к ЗО КИИ. Классы защиты и уровни доверия средств ЗИ	2	2	2	2		Практические и лабораторные задания, тест;
Раздел 2. Представление об этапах создания ЗИС							
4	2.1. Обследование ИС при построении ЗИС. Анализ информационной инфраструктуры и безопасности информации ИС/АС. Архитектура безопасности ИС **Содержание**: Этапы разработки ЗИС и архитектура системы безопасности ИС. Разработка модели угроз и модели нарушителя (с примерами модели угроз БИ в АС). Определение информационной инфраструктуры ИС, подлежащей защите. Определение требуемого класса (уровня) защищенности ИС, их составных частей (в т.ч. АС). Выявление степени участия	4	2	2	2	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;

	персонала в обработке защищаемой информации.						
4	2.2. Этапы жизненного цикла ИС (в т.ч. специфика разработки и эксплуатации ЗИС). Технологии и принципы разработки защищенных ИС. Проблемы безопасности, обусловленные технологиями и подходами к разработке ПС. **Содержание**: Требования стандартов по разработке ПО к безопасности защищенных ИС. Принципы разработки защищенных ИС. Этапы построения системы безопасности ИС. Техзадание на проектирование СЗИ: разработка требований к ЗИС. Аттестация ЗИС (обзорно)	2	2	4	2	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;
5	2.3. Обследование ИС при построении ЗИС **Содержание**: Определение информационной инфраструктуры ИС, подлежащей защите. Анализ требований к назначению, структуре и конфигурации создаваемой автоматизированной системы с целью выявления угроз безопасности информации. Анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите. Классифицирование защищаемой информации по видам тайны и степеням конфиденциальности. Выявление степени участия персонала в обработке защищаемой информации. Классификация и оценка угроз информационной безопасности для объекта информатизации. Разработка модели угроз безопасности информации. Опреде-	2	4	4	2	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;

	ление оценки возможностей внешних и внутренних нарушителей. модель нарушителей в автоматизированных системах. Определение требуемого класса (уровня) защищенности ИС, их составных частей (в т.ч. АС). Определение эффективности применения средств информатизации. Выявление уязвимости информационно-технологических ресурсов ИС/АС						
6	2.4 Показатели надёжности и отказоустойчивости ПО/ИС; средства обеспечения надёжности ПО (резервирование, введение структурной избыточности, протоколирование; модели надёжности программ; алгоритмы автоматического восстановления ИС и т.д.). **Содержание**: Оценка уровня защищенности ИС. Средства обеспечения надёжности ПО. Показатели надёжности и отказоустойчивости ПО/ИС. Защищенный документооборот – обеспечение уровня защищенности ИС (пример ЗИС)	2	2	2	2	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;
7	2.5. Принципы и особенности разработки систем в защищенном исполнении, ЗИС. Проектная, техническая, рабочая, пользовательская документация на ИС. **Содержание**: Стандартизация подходов к обеспечению информационной безопасности; комплексная (интегральная) безопасность ИС. Проблемы (в т.ч. методологические) создания ЗИС. Языковые, программные средства исследования эффективности технологических процессов обработки информации в ИАС. Формали-	2	2	2	3,8	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;

	зация предметной области при создании ИС (и проектировании ЗИС). Разработка и исследование математических моделей процессов. Определение порядка обработки информации в автоматизированной системе. Методологические основы, методы и технологии проектирования, моделирования, исследования систем защиты информации автоматизированных систем. Методы проведения предпроектного обследования, методы проектирования ИАС. Оформление заявки на разработку системы защиты информации автоматизированной системы. Составление технического задания на разработку ИАС (ТЗ на создание подсистем информационной безопасности ИС).						
	Итого за 1 семестр:	***18***	***18***	***18***	***17,8***		
	Раздел 3. Разработка ЗИС. Аттестация ЗИС						
9	3.1. Проектирование ЗИС. Принципы организации документирования разработки, процесса сопровождения программного обеспечения. Средства безопасности в ЗИС. **Содержание:** Структура функциональной и обеспечивающих частей ИАС. Основные функциональные возможности современных систем управления базами данных. Архитектура, основные модели, последовательность и содержание этапов проектирования, физическая организация баз данных. Основные модели данных, модели представления знаний и про-	2	2	2	4	изучение теоретического материала; подготовка к практическим работам	практические и лабораторные задания; опрос; курсовое проектирование

	граммные средства работы с ними. Инфологическая модель предметной области. Общие сведения о методах проектирования, документирования, разработки, тестирования и отладки компонентов обеспечивающей части ИАС. Принципы организации документирования разработки, процесса сопровождения программно го обеспечения.						
10	3.2. Показатели качества и надежности ИС в защищенном исполнении и методы реализации принципов надежности и защищенности. **Содержание:** Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем. Основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации. Особенности защиты информации в АСУ. Исследование аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем. Исследование программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах	2	2	2	4	изучение теоретического материала; подготовка к практическим работам	практические и лабораторные задания; опрос; курсовое проектирование
11	3.3. Разработка ЗИС (часть 1). **Содержание:** Определение структурно-функциональных характеристик информационной системы в соответствии с тре-	2	2	2	4	изучение теоретического материала; подготовка к практическим работам	практические и лабораторные и лабораторные задания; опрос; курсовое проектирование

	бованиями нормативных правовых документов в области защиты информации. Разработка технических заданий на проектирование ИАС Подготовка проектов нормативно-распорядительных документов (приказов, указаний, инструкций) по вопросам создания и эксплуатации ИАС. Подготовка проектной документации на создаваемые ИАС. Проведение технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы. Формирование основных показателей и критериев эффективности ИАС. Формирование разделов технических заданий на создание систем защиты информации автоматизированных систем. Формирование конфигурации и состава обеспечивающей части ИАС. Формирование функциональной части ИАС. Формирование технологии функционирования ИАС. Формирование требований по защите информации, включая использование математического аппарата для решения прикладных задач. Проектирование информационно-лингвистического обеспечения ИАС. Проектирование программного и математического обеспечения ИАС						
12	3.4. Разработка ЗИС (часть 2). **Содержание:** Проектирование технического обеспечения ИАС. Разработка системы защиты информации ИС/АС с учетом действующих нормативно-правовых документов. Разработка проектных доку-	2	2	2	4	изучение теоретического материала; подготовка к практическим работам	практические и лабораторные адания; опрос; курсовое проектирование

	ментов на средства защиты информации создаваемых ИАС. Разработка аналитических и компьютерных моделей автоматизированных систем и подсистем безопасности автоматизированных систем. Проектная и эксплуатационная документация на систему защиты информации. Составление методик тестирования систем защиты информации автоматизированных систем. Определение комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в ИС; состав комплекса средств защиты информации в ИАС.						
Раздел 4. Внедрение и эксплуатация ЗИС.							
13	4.1. Технологии, механизмы и способы обеспечения безопасности в защищенной ИС. **Содержание:** Программно-аппаратные средства обеспечения защиты информации в программном обеспечении автоматизированных систем. Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах. Обоснование необходимости использования криптографических средств защиты информации. Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы. Принципы эксплуатации и сопровождения ЗИС. Содержание и	4	4	2	4	изучение теоретического материала; подготовка к практическим работам	практические и лабораторные задания; опрос/доклад; тест

	порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации. Технико-экономическое обоснование проектных решений обеспечения защиты информации в ИС для обеспечения требуемого уровня защищенности. Администрирование ЗИС. Доступ к данным безопасности. Монитор безопасности, протоколирование, аудит, шифрование, контроль целостности данных, использование электронной цифровой подписи.						
14	Документирование ЗИС. **Содержание:** Проектирование нормативно-распорядительных документов (приказов, указаний, инструкций) по эксплуатации ЗИС. Разработка проектов нормативных документов, регламентирующих работу по защите информации в автоматизированных системах. Проведение анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.	2	2	4	4	изучение теоретического материала; подготовка к практическим работам	практические и лабораторные задания; опрос/доклад; курсовое проектирование, тест
15	4.3. Оценка эффективности ЗИС. **Содержание:** Проведение оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации. Критерии и показатели эффективности СЗИ ИС. Оценка эф-	2	2	2	5,8	изучение теоретического материала; подготовка к практическим работам	практические и лабораторные задания; опрос/доклад; курсовое проектирование, тест

	фективности ЗИС. Разработка предложений по совершенствованию системы управления защиты информации автоматизированных систем. Принципы формирования политики информационной безопасности в автоматизированных системах						
	Итого за 2 семестр:	16	16	16	29,8		
	Всего часов:	**34**	**34**	**34**	**47,6**		