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

Утверждено:
на заседании кафедры
протокол №7 от 18 февраля 2022 г.

Зав. кафедрой /Исмагилова А.С.

Согласовано:
Председатель УМК института

/Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина
Технологии обеспечения информационной безопасности
Б1.О.04

программа магистратуры

Направление
10.04.01 Информационная безопасность

Профиль подготовки
Информационная безопасность цифровых технологий

Квалификация
магистр

Разработчик (составитель)
к.ф.-м.н., доцент

/И.А. Шагапов

Для приема: 2022 г.

Уфа – 2022

Составитель: доцент Шагапов Илдар Ахняфович

Рабочая программа дисциплины утверждена на заседании кафедры протокол от «_18_» _февраля_____ 2022 г. № _7_

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. /

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

Заведующий кафедрой _____/ _____Ф.И.О./

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

Заведующий кафедрой _____/ _____Ф.И.О./

Список документов и материалов

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

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

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.	Знает основные требования к системе обеспечения ИБ; 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.
		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.	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.
		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	Владеет основными методами разработки проекта ТЗ на создание системы обеспечения ИБ; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.
	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	Знает основные требования к техническому проекту подсистемы либо компонента системы обеспечения информационной безопасности
		ОПК-2.2 Умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности

		ОПК-2.3 Владеет основными методами разработки технического проекта системы (подсистемы либо компонента системы) обеспечения информационной безопасности	Владеет основными методами разработки технического проекта системы (подсистемы либо компонента системы) обеспечения информационной безопасности

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Технологии обеспечения информационной безопасности» относится к группе дисциплин обязательной части образовательной программы.

Дисциплина изучается на 2 курсе в 3-4 семестрах.

Целью изучения дисциплины является формирование целостного представления о выборе и обосновании технологий обеспечения информационной безопасности объектов.

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 (зачет)**	
		«Незачтено»	«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.	Знает основные требования к системе обеспечения ИБ; 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.	Не знает основные требования к системе обеспечения ИБ; 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.	Знает основные требования к системе обеспечения ИБ; 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.
ОПК-1.2 Умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке	Умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, специ-	Не умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен	Умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программ-

СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	фикации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	обосновать требования к СОИБ.	ных средств 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	Владеет основными методами разработки проекта ТЗ на создание системы обеспечения ИБ; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Не владеет основными методами разработки проекта ТЗ на создание системы обеспечения ИБ; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Владеет основными методами разработки проекта ТЗ на создание системы обеспечения ИБ; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.

Для экзамена

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Критерии оценивания результатов обучения**			
		«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«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.	Знает основные требования к системе обеспечения ИБ; 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.	Не знает основные требования к системе обеспечения ИБ; 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.	Знает некоторые требования к системе обеспечения ИБ; 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, допускает ошибки	Частично знает основные требования к системе обеспечения ИБ; 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.	Знает основные требования к системе обеспечения ИБ; 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.
ОПК-1.2 Умеет разрабатывать технический проект создания СОИБ	Умеет разрабатывать технический проект создания СОИБ (описание тех-	Не умеет разрабатывать технический проект создания СОИБ (описание техни-	Умеет разрабатывать некоторые элементы технического проекта созда-	Частично умеет разрабатывать технический проект создания СОИБ	Умеет разрабатывать технический проект создания СОИБ (описание тех-

(описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	нических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	ческих решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	ния СОИБ (описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ, допускает ошибки.	(описание технических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	нических решений и мероприятий по подготовке СОИБ, спецификации на комплекс технических и программных средств 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	Владеет основными методами разработки проекта ТЗ на создание системы обеспечения ИБ; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Не владеет основными методами разработки проекта ТЗ на создание системы обеспечения ИБ; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Владеет некоторыми методами разработки проекта ТЗ на создание системы обеспечения ИБ; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта., допускает ошибки	Частично владеет основными методами разработки проекта ТЗ на создание системы обеспечения ИБ; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Владеет основными методами разработки проекта ТЗ на создание системы обеспечения ИБ; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.

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 (зачет)**	
		«Незачтено»	«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	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	Не 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.	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.

его подготовки.	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	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	Не 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	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
ОПК-2.3. Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.	Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.	Не владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.	Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.

Для экзамена

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Критерии оценивания результатов обучения**			
		«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«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.	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.	Не 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.	Знает некоторые 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, . допускает ошибки.	Частично 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.	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.
ОПК-2.2 Умеет выполнять обследо-	Умеет выполнять обследо-	Не умеет выполнять обследова-	Умеет выполнять обследова-	Частично умеет выполнять	Умеет выполнять обследо-

нять обследование/аудит и моделирование предметной области, моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности	вание/аудит и моделирование предметной области, моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ние/аудит и моделирование предметной области, моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ние/аудит и моделирование предметной области, моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности, допускает ошибки.	обследование/аудит и моделирование предметной области, моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности	вание/аудит и моделирование предметной области, моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности
ОПК-2.3. Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.	Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.	Не владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.	Владеет некоторыми навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи, допускает ошибки.	Частично владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.	Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.

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.	Знает основные требования к системе обеспечения ИБ; 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.	Письменная контрольная работа Практическое задание Лабораторная работа
ОПК-1.2 Умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по	Умеет разрабатывать технический проект создания СОИБ (описание технических решений и мероприятий по подготовке СОИБ, специфи-	Письменная контрольная работа Курсовой проект Практическое задание

подготовке СОИБ, спецификации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	кации на комплекс технических и программных средств СОИБ); способен обосновать требования к СОИБ.	Лабораторная работа
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.	Владеет основными методами разработки проекта ТЗ на создание системы обеспечения ИБ; владеет навыками обследования информационного объекта, разработки технического задания на разработку СОИБ объекта.	Письменная контрольная работа Курсовой проект Практическое задание Лабораторная работа

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.	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.	Письменная контрольная работа Курсовой проект Практическое задание Лабораторная работа
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	Умеет выполнять обследование/аудит и моделирование предметной области, моделировать угрозы ИБ; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения ИБ	Письменная контрольная работа Курсовой проект Практическое задание Лабораторная работа
ОПК-2.3. Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.	Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи	Письменная контрольная работа Курсовой проект Практическое задание Лабораторная работа

Критериями оценивания при *модульно-рейтинговой системе* являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (*для экзамена:* текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; *для зачета:* 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)

для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

Рейтинг – план дисциплины

Технологии обеспечения информационной безопасности

Направление подготовки 10.04.01 ИБ

Курс 2, семестр 3

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №1	10	**1**	0	10
Рубежный контроль				
1. Письменная контрольная работа №1	15	1	0	15
1. Лабораторная работа №1	15	1	0	15
Всего				50
Модуль 2.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №2	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №2	15	1	0	15
1. Лабораторная работа №2	15	1	0	15
Всего				50
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Зачет				

Рейтинг – план дисциплины

Технологии обеспечения информационной безопасности

Направление подготовки 10.04.01 ИБ

Курс 2, семестр 4

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 3.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №3	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №3	7	1	0	7
2. Практическая работа №4	8	1	0	8
Всего				35
Модуль 4.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №5	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №3	7	1	0	7
2. Практическая работа №6	8	1	0	8
Всего				35
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Экзамен				30

Экзаменационные билеты

Структура экзаменационного билета: экзаменационный билет содержит 2 теоретических вопроса.

Перечень вопросов для экзамена:

1. Основные требования и рекомендации по защите служебной тайны и персональных
2. данных.
3. Основные рекомендации по защите информации, составляющей коммерческую тайну
4. Классификация технических каналов утечки информации.
5. Понятие информационного сигнала.
6. Модуляция сигналов. Опасные сигналы и их источники.
7. Основные показатели технического канала утечки информации
8. Основные понятия и идеи "Общих критериев". Основные понятия и идеи "Общей
9. методологии оценки безопасности информационных технологий".
10. Классификация функциональных требований безопасности. Классы функциональных требований, описывающие элементарные сервисы безопасности.
11. Классы функциональных требований, описывающие производные сервисы безопасности.
12. Основные понятия и классификация требований доверия безопасности.
13. Оценка профилей защиты и заданий по безопасности.
14. Оценочные уровни доверия безопасности
15. Биометрическая идентификация и аутентификация.
16. Требования к произвольному (дискреционному) управлению доступом.
17. Требования к принудительному (мандатному) управлению доступом.
18. Ролевое управление доступом.
19. Межсетевое экранирование.
20. Системы активного аудита.
21. Анонимизаторы.
22. Выпуск и управление сертификатами.
23. Виртуальные частные сети. Виртуальные локальные сети.
24. Регуляторы безопасности и реализуемые ими цели.
25. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия.
26. Архитектура средств безопасности IP-уровня. Контексты безопасности и управление
27. ключами
28. Обеспечение аутентичности IP-пакетов.
29. Обеспечение конфиденциальности сетевого трафика. Основные идеи и понятия протокола TLS.
30. Протокол передачи записей. Протокол установления соединений и ассоциированные
31. протоколы. Применение протокола HTTP над TLS
32. Общие принципы выработки официальной политики предприятия в области информационной безопасности.
33. Роль поставщика Internet-услуг в реагировании на нарушения безопасности.
34. Меры по защите Internet-сообщества.
35. Маршрутизация, фильтрация и ограничение вещания. Защита системной инфра
36. структуры.
37. Размещение Web-серверов. Возможные вопросы к поставщику Internet-услуг

Образец экзаменационного билета:

…

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

Направление 10.04.01 «Информационная безопасность»
Дисциплина «Технологии обеспечения информационной безопасности»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Концептуальные основы защиты информации
2. Порядок обеспечения защиты информации в АС.

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 при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;

- **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. При выполнении практической части работы допущены несущественные ошибки;

- 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. Студент не решил задачу или при решении допущены грубые ошибки;

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

Комплект контрольных работ

Письменная контрольная работа №1

Вопросы

1. С какой целью создается самостоятельное подразделение по защите информации в организации? Примеры.
2. Что означает аутсорсинг в области информационной безопасности? Примеры.
3. Обязанности руководителя организации в области защиты информации.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	7
Выполнены пункты 1-3	15
Максимальный балл	15

Письменная контрольная работа №2

Вопросы

1. Зайти на сайт ФСТЭК, изучить содержание сайта
2. Выбрать на свое усмотрение 3-4 угрозы и 3-4 уязвимости из предложенного банка
3. Изучить их и подготовить краткий отчет.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	7
Выполнены пункты 1-3	15
Максимальный балл	15

Письменная контрольная работа №3

Вопросы

1. Организационное обеспечение информационной безопасности при проведении закрытых мероприятий.
2. Разработка комплекта документов при организации пропускного режима на предприятии.
3. Основные документы, разрабатываемые на охраняемых объектах.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	3
Выполнены пункты 1-3	7
Максимальный балл	7

Письменная контрольная работа№4

Вопросы

1. Права и обязанности оператора персональных данных.
2. Правовые основания работы с персональными данными.
3. Права субъекта персональных данных.
4. Права и обязанности держателя (обладателя) массивов персональных данных.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	3
Выполнены пункты 1-4	7
Максимальный балл	7

Комплект практических заданий

Для самостоятельного освоения и/или расширения знаний, умений, владений предусмотрены несколько практических заданий.

Типовое практическое задание №1

Модель угроз информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).

2. Собрать необходимую информацию.

3. Построить модель угроз информационной безопасности.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	5
Выполнены пункты 1-3	10
Максимальный балл	10

Типовое практическое задание №2

Модель нарушителя информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).
2. Собрать необходимую информацию.
3. Построить модель нарушителя безопасности.

Методические указания

а. Использовать известные уровни возможностей нарушителя, различные классификации нарушителя.

б. Помнить, для чего строится модель нарушителя.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	5
Выполнены пункты 1-3	10
Максимальный балл	10

Типовое практическое задание №3

Разработка технического задания (ТЗ) в области информационной безопасности

1. Выбрать вариант для написания ТЗ объект (услуга, работа, разработка, модификация и т.д. в области ИБ)
2. Собрать необходимую информацию.
3. Разработать техническое задание.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	5
Выполнены пункты 1-3	10
Максимальный балл	10

Методические указания

а. Изучить ГОСТ по написанию ТЗ и образцы готовых вариантов.

6. Помнить, для чего и для кого разрабатывается ТЗ.

Типовое практическое задание №4

Разработка перечня информации, составляющей коммерческую тайну организации

1. Выбрать (придумать гипотетическую) коммерческую организацию.
2. Изучить деятельность организации.
3. Составить перечень информации (всей), циркулирующей в организации.
4. Провести анализ перечня с фильтрацией информации, имеющей коммерческую ценность для организации.
5. Составить перечень информации, составляющей коммерческую тайну организации

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	4
Выполнены пункты 1-5	8
Максимальный балл	6

Типовое практическое задание №5

Объекты и угрозы информационной безопасности

Цель работы: закрепление умений распознавать на практике угрозы объектам информационной безопасности

1. Выбрать произвольным образом объект обеспечения информационной безопасности.
2. Привести подробное описание объекта.
3. Составить перечень угроз объекту. Произвести классификацию по выбранному признаку.
4. Оценить актуальность этих угроз. Попытаться определить источники этих угроз. Насколько возможно, выявленные угрозы связать с уязвимостями объектов.
5. Составить отчет по работе.

Методические рекомендации по выполнению работы.

При выполнении работы полезно ответить на следующие вопросы:

- Чем руководствовались при составлении перечня угроз?
- Какие преимущества и недостатки имеет выбранная классификация угроз?
- Какова связь между угрозами и уязвимостями?

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	4
Выполнены пункты 1-5	10
Максимальный балл	10

Типовое практическое задание №6

Обеспечение информационной безопасности объекта

Цель работы: закрепление умений обеспечивать информационную безопасность объекта

1. Для объекта из лабораторной работы №3 составить несколько вариантов для противодействия выявленным угрозам .
2. оценить эффективность каждого варианта.
3. Выбрать наиболее эффективный вариант.
4. Подробно расписать, как можно реализовать выбранный вариант противодействия угрозам.
5. Составить отчет по работе.

Методические рекомендации по выполнению работы.

При выполнении работы полезно ответить на следующие вопросы:

- На сколько типичным является объект?
- Из каких соображений были составлены варианты противодействия угрозам?
- На сколько «законным» является наиболее эффективный вариант?
- Что можно сказать, на счет экономической эффективности выбранного варианта?

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	4
Выполнены пункты 1-5	8
Максимальный балл	8

Комплект лабораторных работ

Типовая лабораторная работа №1

Цель работы: закрепление на практике понятия информационная безопасность технической системы

1. Выбрать произвольным образом техническую систему.
2. Привести подробное описание данной технической системы.
3. Расписать максимально подробно, что означает информационная безопасность для данной технической системы. Подобрать типичные примеры, аналогии.
4. Составить отчет по работе.

Методические рекомендации по выполнению работы.

Перед выполнением работы полезно ответить на следующие вопросы:

- Какие сложности возникли при описании технической системы?
- Чем отличается информационная безопасность технической системы от информационной безопасности личности?
- Чем отличается информационная безопасность от защиты информации?:

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	8
Выполнены пункты 1-4	15

Максимальный балл	15

Типовая лабораторная работа №2

Цель работы: закрепление на практике понятия информационная война

1. Группа делится на две подгруппы..
2. Выбирается область (вид) деятельности.
3. Каждая подгруппа выбирает тип «информационного оружия» и разрабатывает план «информационной войны» против другой подгруппы и пытается ее «реализовать», одновременно «защищаясь» от противника.
4. По результатам проводится анализ и «эффективность» действий каждой стороны.
5. Составить отчет по работе каждой подгруппы.

Методические рекомендации по выполнению работы.

При выполнении работы полезно ответить на следующие вопросы:

- Чем руководствовались при выборе информационного оружия?
- Какие методы защиты от информационного оружия противника применялись?
- Что означает эффективность применения информационного оружия?

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	7
Выполнены пункты 1-5	15
Максимальный балл	15

Темы семинарских занятий (3 семестр)

(18 часов)

1. Концептуальные основы защиты информации. Система документов по технической защите информации. Законодательные и иные правовые акты в области технической защиты информации. Сертификация средств защиты информации. Классификация угроз и объектов защиты. Методы оценки опасности угроз. Объект информатизации. Классификация объектов защиты. Классификация информации. Классификация АС. Классификация СВТ.
2. Угрозы несанкционированного доступа к информации. Основные классы атак в сетях на базе TCP/IP. Понятие несанкционированного доступа.
3. Модель потенциального нарушителя. Основные классы атак в сетях на основе TCP/IP.
4. Программно-математическое воздействие. Вредоносные программы и их классификация. Антивирусы. Межсетевой экран.
5. Система обнаружения вторжений. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.
6. Порядок обеспечения защиты информации в АС. Требования и рекомендации в зависимости от типа АС.
7. Защита конфиденциальной информации на автоматизированных рабочих местах. Защита информации в локальных вычислительных сетях.
8. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных.

Критерии оценки (в баллах) *(должны строго соответствовать рейтинг плану по макс. и мин. колич. баллов и только для тех, кто учится с использованием модульно-рейтинговой системы обучения и оценки успеваемости студентов):*

- 0,55 баллов выставляется студенту, если выполнил задание на 100%

- 0,36 баллов выставляется студенту, если выполнил задание на 75%

- 0,2 баллов выставляется студенту, если выполнил задание на 50%

- 0 баллов выставляется студенту, если не выполнил задание

Темы семинарских занятий (4 семестр)

(32 часа)

1. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования. Основные требования и рекомендации по защите служебной тайны и персональных данных.
2. Основные рекомендации по защите информации, составляющей коммерческую тайну.
3. Классификация технических каналов утечки информации.
4. Понятие информационного сигнала. Модуляция сигналов. Опасные сигналы и их источники.
5. Основные показатели технического канала утечки информации. Основные понятия и идеи "Общих критериев". Основные понятия и идеи "Общей методологии оценки безопасности информационных технологий".
6. Классификация функциональных требований безопасности. Классы функциональных требований, описывающие элементарные сервисы безопасности. Классы функциональных требований, описывающие производные сервисы безопасност.
7. Основные понятия и классификация требований доверия безопасности. Оценка профилей защиты и заданий по безопасности.
8. Оценочные уровни доверия безопасности. Биометрическая идентификация и аутентификация.
9. Требования к произвольному (дискреционному) управлению доступом. Требования к принудительному (мандатному) управлению доступом. Ролевое управление доступом.
10. Межсетевое экранирование. Системы активного аудита. Анонимизаторы.
11. Выпуск и управление сертификатами. Виртуальные частные сети. Виртуальные локальные сети.
12. Регуляторы безопасности и реализуемые ими цели. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия.
13. Архитектура средств безопасности IP-уровня. Контексты безопасности и управление ключами. Обеспечение аутентичности IP-пакетов. Обеспечение конфиденциальности сетевого трафика. Основные идеи и понятия протокола TLS.
14. Протокол передачи записей. Протокол установления соединений и ассоциированные протоколы. Применение протокола HTTP над TLS. Общие принципы выработки официальной политики предприятия в области информационной безопасности.
15. Роль поставщика Internet-услуг в реагировании на нарушения безопасности. Меры по защите Internet-сообщества.
16. Маршрутизация, фильтрация и ограничение вещания. Защита системной инфра структуры. Размещение Web-серверов. Возможные вопросы к поставщику Internet-услуг

Критерии оценки (в баллах) *(должны строго соответствовать рейтинг плану по макс. и мин. колич. баллов и только для тех, кто учится с использованием модульно-рейтинговой системы обучения и оценки успеваемости студентов):*

- 0,26 баллов выставляется студенту, если выполнил задание на 100%

- 0,16 баллов выставляется студенту, если выполнил задание на 75%

- 0,1 баллов выставляется студенту, если выполнил задание на 50%

- 0 баллов выставляется студенту, если не выполнил задание

Перечень вопросов для зачета в 3 семестре:

1. Концептуальные основы защиты информации.
2. Система документов по технической защите информации.
3. Законодательные и иные правовые акты в области технической защиты информации.
4. Сертификация средств защиты информации.
5. Классификация угроз и объектов защиты.
6. Методы оценки опасности угроз. Объект информатизации.
7. Классификация объектов защиты. Классификация информации. Классификация АС.
8. Классификация СВТ.
9. Угрозы несанкционированного доступа к информации. Основные классы атак в сетях на базе TCP/IP.
10. Понятие несанкционированного доступа. Модель потенциального нарушителя.
11. Основные классы атак в сетях на основе TCP/IP.
12. Программно-математическое воздействие.
13. Вредоносные программы и их классификация.
14. Антивирусы. Межсетевой экран. Система обнаружения вторжений
15. Требования и рекомендации по защите информации, обрабатываемой средствами
16. вычислительной техники.
17. Порядок обеспечения защиты информации в АС.
18. Требования и рекомендации в зависимости от типа АС.
19. Защита конфиденциальной информации на автоматизированных рабочих местах на
20. базе автономных ПЭВМ.
21. Защита информации в локальных вычислительных сетях.
22. Защита информации при межсетевом взаимодействии.
23. Защита информации при работе с системами управления базами данных.
24. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

Примерная тематика курсовых проектов в 4 семестре по дисциплине

1. Авторское право в интернет-эпоху
2. Административная ответственность как средство обеспечения информационной безопасности.
3. Анализ уязвимостей в области технической защиты информации
4. Аттестация объектов информатизации по требованиям безопасности
5. Вопросы правового обеспечения информационной безопасности в среде Интернет.
6. Государственное регулирование вопросов использования криптографических средств и электронной цифровой подписи.
7. Документация при организации внутриобъектового режима на предприятии.
8. Документация при организации пропускного режима на предприятии.
9. Защита прав, свобод и законных интересов в сфере обеспечения информационной безопасности.
10. Инсайдерская информация: методы борьбы в России и за рубежом.
11. Институт правовой защиты изобретений, полезных моделей, промышленных образцов
12. Институт правовой охраны программ для ЭВМ и баз данных
13. Информационная война в современных условиях
14. Информационные реестры: дилемма безопасности и доступности.
15. Лицензирование в области информационной безопасности.
16. Международное законодательство в области защиты информации.
17. Место органов ФСБ в системе обеспечения информационной безопасности.
18. Методы выявления нарушителей, тактики их действий и состава интересующей их

информации
19. Модели нарушителя информационной безопасности
20. Модели угроз информационной безопасности
21. Мониторинг и анализ данных социальных сетей
22. Направления и виды разведывательной деятельности
23. Неправомерный доступ к компьютерной информации в сетях ЭВМ
24. Обеспечение безопасности критической информационной инфраструктуры
25. Обеспечение информационной безопасности в системе государственной службы.
26. Организационное обеспечение информационной безопасности при проведении закрытых мероприятий.
27. Организационно-правовые вопросы инженерно-технической защиты информации
28. Организационно-правовые вопросы применения полиграфа
29. Организационно-правовые вопросы программно-аппаратной защиты информации
30. Организационно-правовые основы обеспечения информационной безопасности органов государственной власти.
31. Организация внутриобъектового режима.
32. Организация и обеспечение режима секретности на объекте.
33. Организация режима коммерческой тайны предприятия
34. Организация службы информационной безопасности.
35. Основные документы, разрабатываемые на охраняемых объектах.
36. Особенности аудита информационной безопасности
37. Особенности защиты персональных данных
38. Особенности защиты служебной тайны
39. Особенности защиты государственной тайны
40. Особенности защиты информации при проведении конфиденциальных переговоров
41. Особенности защиты коммерческой тайны предприятия
42. Особенности защиты профессиональной тайны
43. Особенности информационных правоотношений, возникающих при производстве, передаче и распространении персональных данных.
44. Особенности обеспечения безопасности Интернета вещей
45. Ответственность при разглашении информации, составляющей коммерческую тайну предприятия
46. Подбор сотрудников и работа с кадрами на предприятии.
47. Подходы к оценке ущерба от нарушений ИБ
48. Правовое регулирование использования электронных документов в Российской Федерации
49. Разработка комплекта документов при проведении аттестационных испытаний защищаемых объектов.
50. Сертификация в области информационной безопасности.
51. Система информационной безопасности предприятия.
52. Совет Безопасности Российской Федерации: правовой статус и положение в системе государственных органов.
53. Современные киберугрозы: способы и методы борьбы.
54. Технические средства охраны источников информации
55. Технологии защищенного документооборота предприятия
56. Управление персоналом, допущенным к конфиденциальной информации
57. Управление рисками информационной безопасности
58. Утечка информации: понятие, виды и организационно-правовые способы борьбы с нею.
59. Уязвимости и угрозы информационной безопасности в области организационной защиты информации
60. Физическая защита информации

61. ФСТЭК в системе обеспечения информационной безопасности.
62. Экономическая эффективность защиты информации

Критерии оценивания курсового проекта

Оценка «отлично»: работа выполнена в полном объеме и изложена грамотным языком в определенной логической последовательности с точным использованием специализированной терминологии; показано уверенное владение прикладными программами.
Оценка «хорошо»: работа выполнена в полном объеме, но имеет один из недостатков: в работе допущены один-два недочета при освещении основного содержания ответа; нет определенной логической последовательности, неточно используется специализированная терминология;
Оценка «удовлетворительно»: работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. Прохорова, О.В. Информационная безопасность и защита информации : учебник [Электронный ресурс] /О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 - ISBN 978-5-9585-0603-3 Режим доступ ; http://biblioclub.ru/index.php?page=book&id=438331
2. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов [Электронный ресурс]. / В.И. Аверченков. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; Режим доступа: http://biblioclub.ru/index.php?page=book&id=93245

Дополнительная литература:

3. Голиков А. М. Защита информации в инфокоммуникационных системах и сетях: учебное пособие[Электронный ресурс]Томский государственный университет систем управления и радиоэлектроники, 2015. -256с. Режим доступа //http:/http://biblioclub.ru/index.php?page=book_red&id=480636&sr=1
4. Сердюк В. А. Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие[Электронный ресурс] Москва: Издательский дом Высшей школы экономики, 2015 .-574с. Режим доступа http://biblioclub.ru/index.php?page=book_red&id=440285&sr=1

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

1. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru.
2. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
3. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
4. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
5. www.fstec.ru –сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.

Перечень лицензионного программного обеспечения:

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.

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
1. Учебная аудитория для проведения занятий лекционного типа: Аудитория № 516. **2. Учебная аудитория для проведения занятий семинарского типа:** Аудитория № 417 Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации. Аудитория № 507. Лаборатория управления информационной безопасностью. **3. Учебная аудитория для курсового проектирования (выполнения курсовых работ):** Аудитория № 613 Аудитория № 608 **5. Учебная аудитория для текущего контроля и промежуточной аттестации:** Аудитория № 609 Адрес всех аудиторий 450076, Республика Башкортостан, Городской Округ Город Уфа, город	Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	**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 **Аудитория № 417. Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.** Оборудование: учебная мебель, доска, комплект учебного оборудования «Блочное кодирование», комплект учебного оборудования «Основы криптографии», учебно-лабораторный стенд «Аттестация объекта информатизации по требованиям защиты от утечек по каналу побочных ЭМИ» **Аудитория № 507. Лаборатория управления информационной безопасностью.** Оборудование: учебная мебель, доска, мультимедиа, комплекс мониторинга WiFi сетей "Зодиак II", универсальный комплект инструментов для проведения работ по специальным проверкам и специальным обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон". **Аудитория № 613** Оборудование: учебная мебель, Персональные компьютеры в комплекте моноблок iRU 502 21.5", моноблоки Lenovo Cseries. **Аудитория № 608** Оборудование: учебная мебель, доска,	**Перечень лицензионного программного обеспечения:** 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.

Уфа, улица Карла Маркса, дом 3/4, помещение 2		мобильное мультимедийное оборудование, телевизор TCL-L55P6US. **Аудитория № 609** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование	

Приложение 1

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

Содержание рабочей программы
дисциплины (3 семестр)

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

Форма контроля:
Зачет 3 семестр

Содержание рабочей программы
дисциплины (4 семестр)

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	51,2
лекций	16
практических/ семинарских	32
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)	20,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	17
Учебных часов на подготовку к экзамену	36

Форма контроля:
Экзамен 4 семестр

3 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР	ЛР	СРС		
1	2	3	4	5	6	7	8
1	Концептуальные основы защиты информации. Система документов по технической защите информации. Законодательные и иные правовые акты в области технической защиты информации. Сертификация средств защиты информации. Классификация угроз и объектов защиты. Методы оценки опасности угроз. Объект информатизации. Классификация объектов защиты. Классификация информации. Классификация АС. Классификация СВТ.	2	2	2	2	Какая информация в организации подлежит обязательному документированию?	Письменная контрольная работа Лабораторная работа Практическое задание
2	Угрозы несанкционированного доступа к информации. Основные классы атак в сетях на базе TCP/IP. Понятие несанкционированного доступа. Модель потенциального нарушителя. Основные классы атак в сетях на основе TCP/IP.	2	2	2	2	С какими уязвимостями связаны угрозы НСД?	Письменная контрольная работа Лабораторная работа Практическое задание
3	Программно-математическое воздействие. Вредоносные программы и их классификация. Антивирусы. Межсетевой экран. Система обнаружения вторжений. Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники. Порядок обеспечения защиты информации в АС. Требования и рекомендации в зависимости от типа АС.	2	2	2	2	Какие основные требования по защите информации, обрабатываемой средствами вычислительной техники?	Письменная контрольная работа Лабораторная работа Практическое задание
4	Защита конфиденциальной информации на автоматизированных рабочих местах. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных.	2	2	2	2	Какая информация подлежит защите на АРМ?	Письменная контрольная работа Лабораторная работа Практическое задание
5	Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования. Основные требования и рекомендации по защите служебной тайны и персональных данных.	2	2	2	2	Какие основные требования и рекомендации по защите служебной тайны?	Письменная контрольная работа Лабораторная работа Практическое задание
6	Основные рекомендации по защите информации, составляющей коммерческую тайну. Классификация технических каналов утечки информации.	2	2	2	2	Какие основные требования и рекомендации по защите коммерческой тайны?	Письменная контрольная работа Лабораторная работа Практическое задание

7	Понятие информационного сигнала. Модуляция сигналов. Опасные сигналы и их источники.	2	2	2	2	Какие основные опасные сигналы и их источники?	Письменная контрольная работа Лабораторная работа Практическое задание
8	Основные показатели технического канала утечки информации. Основные понятия и идеи "Общих критериев". Основные понятия и идеи "Общей методологии оценки безопасности информационных технологий".	2	2	2	2	Для чего нужно выделять показатели каналов утечек конфиденциальной информации?	Письменная контрольная работа Лабораторная работа Практическое задание
9	Классификация функциональных требований безопасности. Классы функциональных требований, описывающие элементарные сервисы безопасности. Классы функциональных требований, описывающие производные сервисы безопасности.	2	2	2	17,8	Для чего вводятся различные виды классификации при защите информации?	Письменная контрольная работа Лабораторная работа Практическое задание
	Всего	18	18	18	17,8		

4 семестр

№	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	СРС		
1	2	3	4	5	6	7	8
10	Основные понятия и классификация требований доверия безопасности. Оценка профилей защиты и заданий по безопасности. Оценочные уровни доверия безопасности. Биометрическая идентификация и аутентификация.	2	4		2	Какая информация в организации подлежит защите?	Письменная контрольная работа Практическое задание
11	Требования к произвольному (дискреционному) управлению доступом. Требования к принудительному (мандатному) управлению доступом. Ролевое управление доступом.	2	4		2	Для чего нужны различные классификации?	Письменная контрольная работа Практическое задание
12	Межсетевое экранирование. Системы активного аудита. Анонимизаторы.	2	4		2	Изучить угрозы безопасности организации	Письменная контрольная работа Практическое задание
13	Выпуск и управление сертификатами. Виртуальные частные сети. Виртуальные локальные сети.	2	4		2	Изучить литературу по коммерческой тайне ор-	Письменная контрольная работа Практическое задание

						ганизации	
14	Регуляторы безопасности и реализуемые ими цели. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия.	2	4		2	Изучить особенности разработки режима коммерческой тайны организации	Письменная контрольная работа Практическое задание
15	Архитектура средств безопасности IP-уровня. Контексты безопасности и управление ключами. Обеспечение аутентичности IP-пакетов. Обеспечение конфиденциальности сетевого трафика. Основные идеи и понятия протокола TLS.	2	4		2,8	Изучить особенности классификации защищаемой информации	Письменная контрольная работа Практическое задание
16	Протокол передачи записей. Протокол установления соединений и ассоциированные протоколы. Применение протокола HTTP над TLS. Общие принципы выработки официальной политики предприятия в области информационной безопасности. Роль поставщика Internet-услуг в реагировании на нарушения безопасности. Меры по защите Internet-сообщества.	2	4		4	Изучить особенности классификации защищаемой информации	Письменная контрольная работа Практическое задание
17	Маршрутизация, фильтрация и ограничение вещания. Защита системной инфра структуры. Размещение Web-серверов. Возможные вопросы к поставщику Internet-услуг	2	4		4	Построить классификацию защищаемой информации для выбранной организации	Письменная контрольная работа Практическое задание
	Итого	16	32		20,8		
	Курсовой проект						Курсовой проект по заданной теме