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

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

Зав. кафедрой _____/Исмагилова А.С.

Согласовано:
Председатель УМК института

_____/Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Защита информации в компьютерных системах и сетях

Б1.О.12
вариативная

программа магистратуры

Направление подготовки
10.04.01 Информационная безопасность

Направленность подготовки
Информационная безопасность цифровых технологий

Квалификация
магистр

Разработчики (составитель)	_____ /А.Ю. Сенцова

Для приема: 2021

Уфа 2021 г.

Составитель / составители: Сенцова А.Ю.

Рабочая программа дисциплины *утверждена* на заседании кафедры управления информационной безопасностью протокол от «_24_» февраля 2021 г. №_8

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

Заведующий кафедрой _____/ _____Ф.И.О./

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

Заведующий кафедрой _____/ _____Ф.И.О./

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

Заведующий кафедрой _____/ _____Ф.И.О./

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 3
2. Цели и место дисциплины в структуре образовательной программы 5
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся) 5
4. Фонд оценочных средств по дисциплине 6
   - 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 6
   - 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. 10
5. Учебно-методическое и информационное обеспечение дисциплины 18
   - 5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины 18
   - 5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы 18
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине 20

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

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 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.
		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.
		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.
	ОПК-2. Способен раз-	ОПК-2.1 Знает основные	Знать основные требова-

	рабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	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.	ния 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 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
		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.

2. Цели и место дисциплины в структуре образовательной программы

Дисциплина «Защита информации в компьютерных системах и сетях» относится к группе дисциплин базовой части образовательной программы магистратуры.

Дисциплина изучается на 1 курсе во 2-м семестре.

Целью учебной дисциплины «Защита информации в компьютерных системах и сетях» является: получение базовых знаний в области теории и практики использования защищенных информационных систем, изучение методики анализа угроз при разработке и эксплуатации защищенных компьютерных систем и сетей, концептуального проектирования защищенных компьютерных систем и сетей; требований к уровню и средствам защиты информации в системах и сетях на основе отечественных и международных стандартов; усвоение требований разработки, предъявляемых к защищенным ИС в условиях современных рисков информационной безопасности, порядок выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности.

.

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 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

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 испол-	Знать 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.	Не знает	В целом 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 , но допускает значительные ошибки.	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, но допускает незначительные ошибки.	Демонстрирует целостность знания основных требовании 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 .

нении; 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.	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.	Не умеет	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, но допускает значительные ошибки.	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, но допускает незначительные ошибки.	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 для решения профессиональных задач обеспечения информационной безопасности.
ОПК-1.3. Владеет основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания	Владеть основными методами разработки проекта технического задания на создание системы обеспечения информационной безопасности; владеет навыками обследования информационного объекта, разработки технического задания на раз-	Не владеет	В целом 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, но допускает	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 , но допускает незначитель-	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 для решения задач профес-

на разработку СОИБ объекта.	работку СОИБ объекта.		значительные ошибки.	ные ошибки.	сиональной деятельности.

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

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 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	В целом 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. , но допускает значительные ошибки.	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. , но допускает незначительные ошибки.	Демонстрирует целостность знании основных требовании 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 обследование/аудит и моделирование предмет-	Уметь выполнять обследование/аудит и моделирование предмет-	Не умеет	Умеет выполнять обследование/аудит и моделирование предметной области,	Умеет выполнять обследование/аудит и моделирование предметной области,	Умеет выполнять обследование/аудит и моделирование предметной области,

ной области, моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ной области, моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности		моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности , но допускает значительные ошибки.	моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности , но допускает незначительные ошибки.	моделировать угрозы информационной безопасности; умеет обосновывать требования к техническому проекту системы (подсистемы либо компонента системы) обеспечения информационной безопасности для решения профессиональных задач обеспечения информационной безопасности.
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.	Не владеет	В целом владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи., но допускает значительные ошибки.	Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи. , но допускает незначительные ошибки.	Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи. для решения задач профессиональной деятельности.

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:* основные правовые нормативные акты, стандарты, нормативные методические документы ФСБ России, ФСТЭК России, регламентирующие разработку информационных систем, обеспечивающих надлежащий уровень информационной защищенности; назначение, состав, функции и возможности автоматизированных различных категорий и классов информационных систем технологии обеспечения информационной безопасности в программах, осуществляющих сбор, обработку, анализ, систематизацию цифровых данных.	Практические задания, лабораторные занятия, тест
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:* применять на практике компьютерные технологии для создания и модернизации систем, средств и технологий обеспечения информационной безопасности	Практические задания, лабораторные занятия, 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:* навыками систематизации, обобщения и анализа данных, необходимых для планирования, модернизации и ввода в эксплуатацию систем и средств обеспечения информационной безопасности, Владеть навыками проектирования ИС, моделирования баз данных для ИС	Практические задания, лабораторные занятия

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

ОПК-2.1. Знает основные	*Знать:* порядок и инструмен-	Практические задания, лабо-

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.	тальные средства разработки и внедрения программного обеспечения и средств обеспечения информационной безопасности.	раторные занятия, 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:* применять основные автоматизированные информационные системы в профессиональной деятельности	Практические задания, лабораторные занятия, тест
ОПК-2.3. Владеет основными навыками использования технологий, методов и средств технического проектирования и моделирования СОИБ с учетом поставленной задачи.	*Владеть:* навыками самостоятельного обучения новым методам исследования в области профессиональной деятельности	Практические задания, лабораторные занятия

Рейтинг – план дисциплины
Защита информации в компьютерных системах и сетях
Направление подготовки 10.04.01 Информационная безопасность
Курс 1, семестр 2

Виды учебной деятельности	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль				**18**
1.Аудиторная работа				
- практические занятия	2	5		10
- лабораторные задания	4	2		8
Рубежный контроль				**5**
тест	5	1	0	5
Всего				**23**
Модуль 2				
Текущий контроль				**23**
1.Аудиторная работа				
- практические занятия	2	4		8
- лабораторные задания	5	3		15
Рубежный контроль				**24**
Тест	24	1		24
Всего				**47**
Поощрительные баллы				
2.Участие в научно-практической конференции по профилю	10	1	0	10
Всего				**10**
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			-6	-6
2. Посещение практических и лабораторных занятий	-	-	-10	-10
Итоговый контроль				
Экзамен			**0**	**30**
ВСЕГО:			0	110 (включая 10 поощр. баллов)

Типовые экзаменационные вопросы

Структура экзаменационного билета: экзаменационный билет содержит 2 теоретических вопроса.

1. Основные понятия в области информационной безопасности.
2. Угрозы нарушения информационной безопасности. Классификация угроз нарушения ИБ
3. Основные типы уязвимостей информационно-вычислительных систем. Этапы жизненного цикла уязвимостей.
4. Уязвимости Spectre и Meltdown.
5. Средства анализа уязвимостей. Проверка заголовков, активные зондирующие проверки, тесты на проникновение.
6. Средства анализа уязвимостей. Этапы сканирования. Сканеры ОС и сканеры сетевого уровня.
7. Подсистема защиты корпоративной сети от вредоносных программ. Сигнатурный и эвристический анализ
8. Эвристические анализаторы
9. Поведенческие блокираторы
10. Встроенные в антивирусные программы межсетевые экраны. Правила для межсетевых экранов антивируса. Способы применения межсетевых экранов для защиты от вредоносных программ.
11. Многоуровневая система защиты информации от вредоносных программ. Виды антивирусных комплексов.
12. Архитектура системы антивирусной защиты на предприятии
13. Классы средств антивирусной защиты. Типы средств антивирусной защиты.
14. Подсистема межсетевого экранирования. Виды межсетевых экранов.
15. Списки управления доступом в межсетевых экранах. Типы списков управления доступом.
16. Правила, которые необходимо соблюдать при построении ACL. Примеры построения списков управления доступом в межсетевых экранах.
17. Списки контроля доступа с дополнительным временным критерием.
18. Зеркальные списки контроля доступа в межсетевых экранах.
19. Динамические списки управления доступом.
20. Шлюзы сеансового уровня. Схема функционирования шлюзов сеансового уровня.
21. Шлюзы прикладного уровня. Схема функционирования прикладных шлюзов.
22. Схемы сетевой защиты на базе межсетевых экранов. Схема с использованием экранирующего маршрутизатора и схема единой защиты ЛВС
23. Схемы сетевой защиты на базе межсетевых экранов. Схема с защищаемой закрытой и не защищаемой открытой подсетями
24. Схемы сетевой защиты на базе межсетевых экранов. Схема с раздельной защитой закрытой и открытой подсетей.
25. Жизненный цикл атаки. Внешняя разведка
26. Жизненный цикл атаки. Сканирование системы. Программы Nmap, Metasploit, John the Ripper
27. Жизненный цикл атаки. Сканирование системы. Программы TCP Hydra, Wireshark, Aircrack-ng, Cain and Abel.
28. Жизненный цикл атаки. Повышение привилегий.

29. Жизненный цикл атаки. Эксфильтрация. Осуществление деструктивных воздействий на систему.
30. Жизненный цикл атаки. Обфускация.
31. Распространение атаки по сети. Виды сканирования. SYN-сканирование.
32. Распространение атаки по сети. Виды сканирования. TCP-сканирование и UDP-сканирование.
33. Вариант доступа к ресурсам организации «Защищенная ДМЗ»
34. ДМЗ с разделением сервисов на Front-End и Back-End
35. Демилитаризованная зона, определение, ее цель и суть. Правила фильтрации, которые должны быть установлены в политике межсетевого экранирования в простой ДМЗ
36. Вариант доступа к сервисам организации «Плоская сеть»
37. Преимущества и недостатки использования ДМЗ на предприятии.
38. Механизм ролевого разграничения доступа к командам маршрутизатора
39. Методы защиты учетных записей администратора и пользователей
40. Угрозы нарушения безопасности маршрутизации сети и основные методы защиты инфраструктуры маршрутизации в сети
41. Механизмы и средства обеспечения отказоустойчивости и масштабирования на основе протокола OSPF.
42. Использование VLAN для защиты конфиденциальных данных в сети. Пример построения маршрутизируемых VLAN, в которых используется устройства компании Cisco
43. Принципы, используемые при создании и настройке защищенных коммутируемых ЛВС
44. Реализация атаки VLAN Hopping. Методика проведения атаки, методы защиты от атаки.
45. Протокол VTP с точки зрения информационной безопасности. Принцип работы протокола, режимы работы, безопасность протокола.
46. Скрытие топологии сети с помощью функции трансляции сетевых адресов.

Образец билета:

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

Направление подготовки 10.04.01 «Информационная безопасность»

Дисциплина: Защита информации в компьютерных системах и сетях

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 20

1. Угрозы нарушения информационной безопасности. Классификация угроз нарушения ИБ
2. Преимущества и недостатки использования ДМЗ на предприятии.

Зав. кафедрой УИБ А.С. Исмагилова
Кафедра управления информационной безопасностью

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

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

Критерии оценивания результатов экзамена:

Критерии оценки (в баллах):

- 25-30 баллов выставляется, если обучающийся дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Обучающийся без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;

- 17-24 баллов выставляется, если обучающийся 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, если при ответе на теоретические вопросы 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. Обучающийся не решил задачу или при решении допущены грубые ошибки;

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

Типовые задания для практических занятий

Модуль 1. Информационные системы. Угрозы информационной безопасности, реализуемые с применением ИС. Представление о защищенных ИС

Практическое занятие 1. Защита от атак канального уровня

Цель: знакомство с различными методами атак канального уровня модели OSI

Содержание: организовать фильтрацию портов коммутаторов в соответствии с заданием:

1. Статическое назначение списка портов.
2. Динамическое назначение списка портов.
3. Организация атаки MAC-flood и защита от такой атаки.
4. Организация атаки MAC-spoofing и защита от такой атаки.
5. Организация варианта реагирования на атаки shutdown.
6. Организация варианта реагирования на атаки protect.
7. Организация варианта реагирования на атаки restrict.

Методические рекомендации:

Методические рекомендации для выполнения настроек безопасности и проведения атак канального уровня предоставляются студентам в электронном виде преподавателем на занятии. Все настройки безопасности и атаки, в особенности те, которые включают в себя проведения тестов на проникновение с целью деструктивного воздействия на систему, проводятся только на виртуальном оборудовании с применением эмуляции информационно-телекоммуникационного оборудования.

Критерии и методика оценивания результатов семинарского занятия №1:
- 1 балл выставляется, если работа выполнена с ошибками и/или поставленная в задаче цель достигнута частично (наполовину);
- 2 балла выставляется, если работа занятия выполнена без ошибок и без замечаний.

И т.д. Подробнее см. в фонде оценочных средств

Типовые задания для выполнения лабораторных работ

Модуль 1. Информационные процессы. Информационные системы

Лабораторное занятие №1. Изучение основных способов и методов защиты учетных записей в операционных системах сетевого оборудования

Цель: изучение стандартных встроенных механизмов защиты учетных записей пользователей и администраторов сети в информационно-телекоммуникационном оборудовании.

Содержание лабораторной работы:

1. Построить небольшую информационную систему в эмуляторе.
2. Определить, какое оборудование будет настраиваться в ходе лабораторной работы с помощью терминального клиента и консоли администратора.
3. Выполнить настройку, разработать шаблоны конфигурационных файлов.
4. Предложить набор учетных записей и прав доступа для эксплуатации телекоммуникационного оборудования в корпоративной сети.

Методические рекомендации:
Методические рекомендации для выполнения настроек безопасности предоставляются студентам в электронном виде преподавателем на занятии. Все настройки безопасности проводятся только на виртуальном оборудовании с применением эмуляции информационно-телекоммуникационного оборудования.

И т.д. Подробнее см. в фонде оценочных средств

Критерии и методика оценивания результатов лабораторных занятий:
- 1-2 балл выставляется, если работа выполнена с ошибками и/или поставленная в задаче цель достигнута частично (на одну треть верно);
- 3 балла выставляется, если работа занятия выполнена с мелкими ошибками или наполовину и более верно.
- 4-5 баллов – если задания лабораторной работы сделаны полно, вовремя и верно (в 1 модуле максимальный балл за одну лабораторную работу равен, максимум, 4-м, во втором модуле – 5-и).

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 письменной форме или в системе дистанционного тестирования.

1 Чем угроза нарушения ИБ отличается от атаки?

1) Угроза совершается внутренним источником угроз, а атака внешним;
2) Угроза - это реализованная атака;
3) Атака - это реализованная угроза.

2 В соответствии с классификацией угроз угрозу раскрытия параметров системы называют _____ угрозой нарушения ИБ, а угрозу нарушения конфиденциальности _____ угрозой нарушения ИБ (вставьте правильное)

3 Как называется программа, которая ищет/использует уязвимости систем для реализации атаки?

1) Ревизор;
2) Сканер;
3) Эксплоит.

4 Какой из видов уязвимостей является самым опасным и трудно исправимым?

1) Уязвимости эксплуатации;
2) Уязвимости проектирования;
3) Уязвимости реализации.

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

Критерии оценки тестовых заданий для ОФО

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (10 вопросов)	Неправильный ответ / Правильный ответ	0/1

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная учебная 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 учебная 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. ГарифуллинаС.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

1. Электронная библиотечная система БашГУ – www.bashlib.ru
2. Электронная библиотечная система «ЭБ БашГУ» - https://elib.bashedu.ru/
3. Электронная библиотечная система «Университетская библиотека онлайн» - https://biblioclub.ru/
4. Электронная библиотечная система издательства «Лань» - https://e.lanbook.com/
5. Электронный каталог Библиотеки БашГУ - http://www.bashlib.ru/catalogi/ -

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. Лицензиибессрочные.
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).GNUGeneralPublicLicense. Лицензии бессрочные.

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 № 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 Аудитория № 613 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/1	практические занятия	**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. Специализированная аудитория с лабораторным оборудованием.** 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. **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.

3. Учебная аудитория для проведения групповых и индивидуальных консультаций: Аудитория № 608 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/1	Консультации	**Аудитория № 608** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, телевизор TCL-L55P6US.
4. Учебная аудитория для текущего контроля и промежуточной аттестации Аудитория № 609 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/1	текущий контроль, промежуточная аттестация	**Аудитория № 609** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование

Приложение 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Содержание рабочей программы
дисциплины «Защита информации в компьютерных системах и сетях»
на 2 семестр ОФО

Вид работы	Объем дисциплины
	ОФО
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часа
Учебных часов на контактную работу с преподавателем:	49,2
Лекций	16
Практических/ семинарских	16
Лабораторных	16
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	13,8
Учебных часов на подготовку к экзамену (Контроль)	45

Форма контроля
Экзамен 2 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 / Сем	ЛР	СРС		
1	2	3	4	5	6	7	8
	Модуль 1. Информационные процессы. Информационные системы						
1	**Тема 1. Информационные системы. Основные понятия и определения в области ИБ. Угрозы нарушения информационной безопасности** **Содержание:** Защита информации, информационная безопасность. Злоумышленник и нарушитель. Утечка и несанкционированный доступ к информации. Модели безопасности. Банк угроз информационной безопасности ФСТЭК. Международная база данных уязвимостей (NVD). Доктрина информационной безопасности РФ. Угрозы и уязвимости электронной торговой площадки и электронных аукционов. Угрозы и уязвимости технологии виртуализации. Защита ЛВС от петель на канальном уровне. Понятие угроз нарушения информационной безопасности, их классификация. Понятие атаки и модели угроз, понятие политики обеспечения ИБ. Атака "отказ в обслуживании"	2	2		1,8	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, подготовка к практическому занятию	ПР, ЛР
2	**Тема 2. Основные типы уязвимостей ИС, этапы жизненного цикла уязвимостей, способы и методы анализа уязвимостей, сканеры уязвимостей** **Содержание:** Методы классификации и оценивания	2	2		2	Самостоятельное изучение рекомендуемой основной и дополнительной	ПР, ЛР

	угроз безопасности информации для объекта информатизации. Классификация уязвимостей по источнику возникновения. Аппаратные уязвимости процессоров и способы их эксплуатации. Эксплоиты, анализ уязвимостей автоматизированных систем. Средства анализа уязвимостей. Анализ заголовков, активные зондирующие проверки, тесты на проникновение. Жизненный цикл уязвимостей. Этапы сканирования уязвимостей. Сканеры операционных систем. Жизненный цикл атаки.					литературы, подготовка к практическому занятию	
3	**Тема 3. Подсистема защиты корпоративной сети от вредоносных программ** **Содержание:** Принципы построения антивирусного программного обеспечения. Сигнатуры, состав базы сигнатур антивирусного программного обеспечения. Эвристические методы защиты: эвристические анализаторы, поведенческие блокираторы, буфер эмуляции. Локации вирусного ПО, компоненты и вспомогательное программное обеспечение антивирусных средств защиты. Тестирование работы антивируса, создание тестового вируса. Встроенные в антивирусные программы межсетевые экраны. Многоуровневая система защиты информации от вредоносных программ. Типы и классы антивирусных комплексов в соответствии с нормативными документами ФСТЭК РФ.	2	2	4	2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	ПР, ЛР
4	**Тема 4. Подсистема межсетевого экранирования в компьютерной системе**. **Содержание:** Принципы построения межсетевых экранов. Виды межсетевых экранов. Списки управления доступом. Построение списков управления доступом в межсетевых экранах, администрирование маршрутизатора со встроенным межсетевом экраном. Правила для по-	4	4	4	2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, подготовка к	ПР, ЛР, Т

	строения списков управления доступом. Политика разграничения доступа в маршрутизаторах и межсетевых экранах. Временной параметр при построении списка управления доступом, динамические и зеркальные списки управления доступом. AAA при конфигурировании динамических списков. Технология трансляции IP-адресов. Изоляция сегментов сети. Шлюзы прикладного уровня, посредники приложений. Схемы сетевой защиты на базе межсетевых экранов.					практическому и лабораторному занятию	
	Модуль 2. Разработка защищенных ИС. Обеспечение безопасности ИС						
5	**Тема 5. Жизненный цикл атаки.** **Содержание:** Внешняя разведка, сканирование сети и портов, повышение привилегий, эксфильтрация, деструктивное воздействие на систему, обфускация.	4	4	4	3	Самостоятельное изучение литературы	ПР, ЛР
6	**Тема 6. Компрометация системы, поиск точки входа в периметр системы. Методы повышения привилегий в различных операционных системах** **Содержание:** Построение системы защиты информации с помощью межсетевого экрана Cisco ASA Компрометация системы, поиск точек входа в сеть Компрометация web-приложений. Виды компрометации операционных систем. Полезные нагрузки. Методы горизонтального повышения привилегий. Методы вертикального повышения привилегий.	2	2	4	3	Самостоятельное изучение литературы	ПР, ЛР, Т
	Всего	16	16	16	13,8		