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

Дисциплина
Информационная безопасность автоматизированных систем

Часть, формируемая участниками образовательных отношений (Б1.В.04)

программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация
«Организация и технологии защиты информации (по отраслям)»

Квалификация
специалист по защите информации

Разработчик (составитель) ._____.	_____/ Салов И.В.

Для приема: 2022г.

Уфа 2022 г.

Составитель: Салов Игорь Владимирович

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 4
2. Цель 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 5

   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. 5

   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. 11
5. Учебно-методическое и информационное обеспечение дисциплины 34

   5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины 34

   5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы 35
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине 37

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

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций (при наличии ОПК)	**Формируемая компетенция (с указанием кода)**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения по дисциплине**
Организационно-управленческая	ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей.	ПК-1.1 Знает основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Знать основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.
		ПК-1.2 Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Уметь применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.
		ПК-1.3 Владеет методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеть методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.
Эксплуатационная	ПК-2. Способен проводить мероприятия по оценке защищенности компьютерных систем и сетей.	ПК-2.1 Знает основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	Знать основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.
		ПК-2.2 Умеет проводить мероприятия по оценке защищенности компьютерных систем и сетей.	Уметь проводить мероприятия по оценке защищенности компьютерных систем и сетей.
		ПК-2.3 Владеет методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.	Владеть методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.

Проектно-технологические	ПК-4. Способен определять основные угрозы безопасности информации в автоматизированных системах.	ПК-4.1 Знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах.	Знать принципы и методы определения основные угроз безопасности информации в автоматизированных системах.
		ПК-4.2 Умеет определять основные угрозы безопасности информации в автоматизированных системах.	Уметь определять основные угрозы безопасности информации в автоматизированных системах.
		ПК-4.3 Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах.	Владеть принципами и методами определения основные угроз безопасности информации в автоматизированных системах.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность автоматизированных систем» относится к обязательной части.

Дисциплина изучается на 4 курсе в 7,8 семестрах.

Целью учебной дисциплины «Информационная безопасность автоматизированных систем», является формирование навыков определения основных угрозы безопасности информации в автоматизированных системах, проведения мероприятий по оценке защищенности компьютерных систем и сетей и формировать требования по защите информации и политики безопасности компьютерных систем и сетей.

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

ПК-1.Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК-1.1 Знает основные принципы, методы и этапы формирования требования по защите	Знать основные принципы, методы и этапы формирования требования по защите	Не знает или показывает очень слабые	Знает некоторые основные принцип	Знает некоторые основные принцип	Знает основные принципы, методы и

информации и политики безопасности компьютерных систем и сетей.	информации и политики безопасности компьютерных систем и сетей.	знания.	ы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей, но допускает ошибки при их применении.	ы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.
ПК-1.2 Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Уметь применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Не умеет.	Умеет применять некоторые основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей., но допускает ошибки при их применении.	Умеет применять некоторые основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.
ПК-1.3 Владеет методикой формирования требований по защите информации и политики безопасности	Владеть методикой формирования требований по защите информации и политики безопасности компьютерных систем и	Не владеет.	Владеет основными элементами методики формиро	Владеет основными элементами методики формиро	Владеет методикой формирования требований по

компьютерных систем и сетей.	сетей.		вания требований по защите информации и политики безопасности компьютерных систем и сетей, но допускает ошибки при их использовании.	вания требований по защите информации и политики безопасности компьютерных систем и сетей.	защите информации и политики безопасности компьютерных систем и сетей.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ПК-1.1 Знает основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Знать основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Не знает или показывает очень слабые знания.	Знает основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.
ПК-1.2 Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Уметь применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Не умеет.	Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.
ПК-1.3 Владеет методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеть методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Не владеет.	Владеет методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.

ПК-2.Способен проводить мероприятия по оценке защищенности компьютерных систем и сетей.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК-2.1 Знает основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	Знать основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	Не знает или показывает очень слабые знания.	Знает некоторые основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения, но делает ошибки при их выборе.	Знает некоторые основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	Знает основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.
ПК-2.2 Умеет проводить мероприятия по оценке защищенности компьютерных систем и сетей.	Уметь проводить мероприятия по оценке защищенности компьютерных систем и сетей.	Не умеет.	Умеет проводить основные мероприятия по оценке защищенности компьютерных систем и сетей, но делает ошибки при их использовании.	Умеет проводить основные мероприятия по оценке защищенности компьютерных систем и сетей.	Умеет проводить мероприятия по оценке защищенности компьютерных систем и сетей.
ПК-2.3 Владеет методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.	Владеть методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.	Не владеет.	Владеет основными методами и принципами проведения мероприятия по	Владеет основными методами и принципами проведения мероприятия по	Владеет методами и принципами проведения мероприятия по оценке защищен

			оценке защищенности компьютерных систем и сетей, но делает ошибки при их использовании.	оценке защищенности компьютерных систем и сетей.	ности компьютерных систем и сетей.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ПК-2.1 Знает основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	Знать основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	Не знает или показывает очень слабые знания.	Знает основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.
ПК-2.2 Умеет проводить мероприятия по оценке защищенности компьютерных систем и сетей.	Уметь проводить мероприятия по оценке защищенности компьютерных систем и сетей.	Не умеет.	Умеет проводить мероприятия по оценке защищенности компьютерных систем и сетей.
ПК-2.3 Владеет методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.	Владеть методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.	Не владеет.	Владеет методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.

ПК-4.Способен определять основные угрозы безопасности информации в автоматизированных системах.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК-4.1 Знает принципы и методы определения основные угроз безопасности информации в автоматизированных	Знать принципы и методы определения основные угроз безопасности информации в автоматизированных	Не знает или показывает очень слабые знания.	Знает основные принципы и методы определения	Знает основные принципы и методы определения	Знает принципы и методы определения основные

системах.	системах.		основные угроз безопасности информации в автоматизированных системах, но делает ошибки при их выборе.	основные угроз безопасности информации в автоматизированных системах.	угроз безопасности информации в автоматизированных системах.
ПК-4.2 Умеет определять основные угрозы безопасности информации в автоматизированных системах.	Уметь определять основные угрозы безопасности информации в автоматизированных системах.	Не умеет.	Умеет определять некоторые основные угрозы безопасности информации в автоматизированных системах, но совершает при этом ошибки.	Умеет определять некоторые основные угрозы безопасности информации в автоматизированных системах.	Умеет определять основные угрозы безопасности информации в автоматизированных системах.
ПК-4.3 Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах.	Владеть принципами и методами определения основные угроз безопасности информации в автоматизированных системах.	Не владеет.	Владеет основными принципами и методами определения основные угроз безопасности информации в автоматизированных системах, но делает ошибки при их использовании.	Владеет основными принципами и методами определения основные угроз безопасности информации в автоматизированных системах.	Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ПК-4.1 Знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах.	Знать принципы и методы определения основные угроз безопасности информации в автоматизированных системах.	Не знает или показывает очень слабые знания.	Знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах.
ПК-4.2 Умеет определять основные угрозы безопасности информации в автоматизированных системах.	Уметь определять основные угрозы безопасности информации в автоматизированных системах.	Не умеет.	Умеет определять основные угрозы безопасности информации в автоматизированных системах.
ПК-4.3 Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах.	Владеть принципами и методами определения основные угроз безопасности информации в автоматизированных системах.	Не владеет.	Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах.

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

ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ПК-1.1 Знает основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Знать основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	тестирование, практическое задание
ПК-1.2 Умеет применять основные принципы, методы и этапы	Уметь применять основные принципы, методы и этапы формирования требования по	тестирование, практическое задание

формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	защите информации и политики безопасности компьютерных систем и сетей.	
ПК-1.3 Владеет методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеть методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	тестирование, практическое задание

ПК-2.Способен проводить мероприятия по оценке защищенности компьютерных систем и сетей.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ПК-2.1 Знает основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	Знать основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	тестирование, практическое задание
ПК-2.2 Умеет проводить мероприятия по оценке защищенности компьютерных систем и сетей.	Уметь проводить мероприятия по оценке защищенности компьютерных систем и сетей.	тестирование, практическое задание
ПК-2.3 Владеет методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.	Владеть методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.	тестирование, практическое задание

ПК-4.Способен определять основные угрозы безопасности информации в автоматизированных системах.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ПК-4.1 Знает принципы и методы определения основные угроз безопасности информации в автоматизированных системах.	Знать принципы и методы определения основные угроз безопасности информации в автоматизированных системах.	тестирование, практическое задание
ПК-4.2 Умеет определять основные угрозы безопасности	Уметь определять основные угрозы безопасности информации в	тестирование, практическое задание

информации в автоматизированных системах.	автоматизированных системах.	
ПК-4.3 Владеет принципами и методами определения основные угроз безопасности информации в автоматизированных системах.	Владеть принципами и методами определения основные угроз безопасности информации в автоматизированных системах.	тестирование, практическое задание

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 экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

для зачета:

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

не зачтено – от 0 до 59 рейтинговых баллов).

Рейтинг – план дисциплины
«Информационная безопасность автоматизированных систем»

Специальность: 10.05.05 Безопасность информационных технологий в правоохранительной сфере

курс 4, семестр7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Общая характеристика информационной защиты автоматизированных систем.				
Текущий контроль			0	
Практическая работа	4	9	0	36
Рубежный контроль				
Тест	14	1	0	14
Всего			0	50
Модуль 2. Организационная структура системы обеспечения безопасности автоматизированных систем.				
Текущий контроль				
Практическая работа	4	9	0	36
Рубежный контроль				
Тест	14	1	0	14
Всего			0	50
Поощрительные баллы				

1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10
Итоговый контроль				
1. Зачет	60	1	60	100

курс 4, семестр 8

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 3. Обеспечение безопасности АС.				
Текущий контроль				
Практическая работа	7	4	0	28
Рубежный контроль				
Тест	12	1	0	12
Всего			0	40
Модуль 4. Уязвимости АС.				
Текущий контроль				
Практическая работа	5	4	0	20
Рубежный контроль				
Тест	10	1	0	10
Всего			0	30
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10
Итоговый контроль				
1.Экзамен	30	1	0	30

Зачет

Вопросы для зачета:

1. Особенности современных автоматизированных систем как объектов защиты.

2. Основные понятия в области безопасности автоматизированных систем
3. Определение безопасности автоматизированных систем.
4. Информация и информационные ресурсы.
5. Субъекты информационных отношений, их безопасность.
6. Цель защиты автоматизированной системы и циркулирующей в ней информации.
7. Угрозы безопасности автоматизированных систем
8. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем.
9. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений.
10. Классификация угроз безопасности.
11. Классификация каналов проникновения в автоматизированную систему и утечки информации.
12. Неформальная модель нарушителя.
13. Меры и основные принципы обеспечения безопасности автоматизированных систем
14. Виды мер противодействия угрозам безопасности.
15. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.
16. Правовые основы обеспечения безопасности автоматизировании систем
17. Защищаемая информация.
18. Лицензирование.
19. Сертификация средств защиты информации и аттестация объектов информатизации.
20. Специальные требования и рекомендации по технической защите конфиденциальной информации.
21. Юридическая значимость электронных документов с электронной подписью.
22. Ответственность за нарушения в сфере защиты информации.
23. Государственная система защиты информации
24. Главные направления работ по защите информации.
25. Структура государственной системы защиты информации.
26. Организация защиты информации в системах и средствах информатизации и связи.
27. Контроль состояния защиты информации.
28. Финансирование мероприятий по защите информации.
29. Организационная структура системы обеспечения безопасности автоматизированных систем
30. Технология управления безопасностью информации и ресурсов в автоматизированной системе.
31. Институт ответственных за обеспечение информационной безопасности.
32. Регламентация действий пользователей и обслуживающего персонала автоматизированной системы.
33. Политика безопасности организации.
34. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

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

не зачтено – от 0 до 59 рейтинговых баллов).

Экзамен

Структура экзаменационного билета

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

Экзаменационные материалы

1. Распределение функций по обеспечению безопасности автоматизированных систем.
2. Организационно-распорядительные документы по обеспечению безопасности автоматизированных систем.
3. Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях
4. Проблема человеческого фактора.
5. Общие правила обеспечения безопасности.
6. Обязанности ответственного за обеспечение безопасности информации в подразделении.
7. Ответственность за нарушения требований обеспечения безопасности.
8. Порядок работы с носителями ключевой информации.
9. Регламентация работ по обеспечению безопасности автоматизированных систем
10. Регламентация правил парольной и антивирусной защиты.
11. Регламентация порядка допуска к работе и изменения полномочий пользователей автоматизированной системы.
12. Регламентация порядка изменения конфигурации аппаратно-программных средств автоматизированной системы.
13. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач.
14. Категорирование и документирование защищаемых ресурсов ....
15. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов.
16. Категорирование защищаемых ресурсов.
17. Проведение информационных обследований и документирование защищаемых ресурсов.
18. Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем автоматизированной системы.
19. Концепция информационной безопасности организации.
20. План защиты информации.
21. План обеспечения непрерывной работы и восстановления подсистем автоматизированной системы.
22. Назначение и возможности средств защиты информации от несанкционированного доступа.
23. Основные механизмы защиты автоматизированных систем.
24. Защита периметра компьютерных сетей и управление механизмами защиты.
25. Страхование информационных рисков.
26. Аппаратно-программные средства защиты информации от несанкционированного доступа.
27. Рекомендации по выбору средств защиты информации от несанкционированного доступа.

28. Обзор существующих на рынке средств защиты информации от несанкционированного доступа.
29. Средства аппаратной поддержки.
30. Способы аутентификации.
31. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа
32. Стратегия безопасности Microsoft.
33. Защита от вмешательства в процесс нормального функционирования автоматизированной системы.
34. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы.
35. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа.
36. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.
37. Обеспечение безопасности компьютерных сетей.
38. Проблемы обеспечения безопасности в компьютерных сетях.
39. Типовая корпоративная сеть.
40. Уровни информационной инфраструктуры корпоративной сети.
41. Уязвимости и их классификация.
42. Классификация атак.
43. Средства защиты сетей.
44. Защита периметра корпоративной сети.
45. Угрозы, связанные с периметром корпоративной сети.
46. Составляющие защиты периметра.
47. Межсетевые экраны.
48. Анализ содержимого почтового и веб-трафика.
49. Виртуальные частные сети.
50. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности.
51. Управление уязвимостями.
52. Архитектура систем управления уязвимостями.
53. Особенности сетевых агентов сканирования.
54. Средства анализа защищенности системного уровня.
55. Мониторинг событий безопасности
56. Введение в управление журналами событий.
57. Категории журналов событий.
58. Инфраструктура управления журналами событий.
59. Введение в технологию обнаружения атак.
60. Классификация систем обнаружения атак.

Пример экзаменационного билета:

Форма 1.4.-33

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ
КАФЕДРА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Дисциплина Информационная безопасность автоматизированных систем

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Распределение функций по обеспечению безопасности автоматизированных систем.
2. Защита периметра компьютерных сетей и управление механизмами защиты.

Зав. Кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии оценивания результатов экзамена для ОФО:

Критерии оценки (в баллах):

- 25-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание терминологии, основных понятий, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы.
- 17-24 баллов выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности.
- 10-16 баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос.
- 1-10 баллов выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

Экзамены:

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

Примерная тематика курсовых проектов (работ)

Курсовое проектирование не предусмотрено

Тестовые задания

При изучении дисциплины используются тестовые задания закрытого типа. Каждое тестовое задание включает вопрос и варианты ответов к нему. Тестирование выполняется в письменной форме.

Необходимо выбрать один ответ из предложенных вариантов.

Модуль 1. Общая характеристика информационной защиты автоматизированных систем

1) С точки зрения ГТК основной задачей средств безопасности является обеспечение:
   а) сохранности информации
   б) **защиты от НСД**
   в) простоты реализации
   г) надежности функционирования
2) Согласно «Оранжевой книге» дискреционную защиту имеет группа критериев
   а) D
   б) A
   в) B
   г) **C**
3) При качественном подходе риск измеряется в терминах
   а) денежных потерь
   б) **заданных с помощью шкалы или ранжирования**
   в) оценок экспертов
   г) объема информации
4) При полномочной политике безопасности совокупность меток с одинаковыми значениями образует
   а) область равной критичности
   б) область равного доступа
   в) **уровень безопасности**
   г) уровень доступности
5) Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это
   а) уязвимость информации
   б) надежность информации
   в) защищенность информации
   г) **безопасность информации**
6) Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это
   а) аудит
   б) **аутентификация**
   в) авторизация
   г) идентификация
7) Согласно «Оранжевой книге» уникальные идентификаторы должны иметь
   а) наиболее важные субъекты
   б) наиболее важные объекты
   в) **все субъекты**
   г) все объекты
8) Соответствие средств безопасности решаемым задачам характеризует
   а) эффективность
   б) корректность
   в) адекватность
   г) унификация
9) Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется
   а) актуальностью информации
   б) доступностью
   в) **качеством информации**
   г) целостностью

10) Конкретизацией модели Белла-ЛаПадула является модель политики безопасности
    а) LWM
    б) На основе анализа угроз
    в) Лендвера
    г) С полным перекрытием
11) Недостатком модели конечных состояний политики безопасности является
    а) изменение линий связи
    б) статичность
    в) **сложность реализации**
    г) низкая степень надежности
12) Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется
    а) избирательным
    б) **мандатным**
    в) привилегированным
    г) идентифицируемым
13) Организационные требования к системе защиты
    а) управленческие и идентификационные
    б) административные и аппаратурные
    в) **административные и процедурные**
    г) аппаратурные и физические
14) При избирательной политике безопасности в матрице доступа на пересечении столбца и строки указывается
    а) тип разрешенного доступа
    б) субъект системы
    в) факт доступа
    г) объект системы
15) Основу политики безопасности составляет
    а) программное обеспечение
    б) управление риском
    в) **способ управления доступом**
    г) выбор каналов связи
16) Идентификация и аутентификация пользователей, управление доступом, протоколирование и аудит, криптография, экранирование и обеспечение высокой доступности:
    а) процедурному уровню;
    б) законодательному уровню;
    в) административному уровню;
    г) **программно-техническому уровню.**
17) Управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ, относятся к :
    а) процедурному уровню;
    б) законодательному уровню;
    в) административному уровню;
    г) программно-техническому уровню.
18) Слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы, называется:
    а) Источником угрозы;
    б) Окном опасности;
    в) **Уязвимость;**
    г) Критичностью реализации угрозы.
19) Модель угроз это :

а) документ, определяющий перечень и характеристики основных (актуальных) угроз безопасности и уязвимостей при их обработке в ИС, которые должны учитываться в процессе организации защиты информации, проектирования и разработки систем защиты информации, проведения проверок (контроля) защищенности ИС;

б) совокупность документированных руководящих принципов, правил, процедур и практических приёмов в области ИБ, которые регулируют управление, защиту и распределение ценной информации;

в) комплекс политических, правовых, экономических, социально-культурных и организационных мероприятий государства, направленный на обеспечение конституционного права граждан на доступ к информации;

г) Нет правильного ответа.

20) Через уязвимость «Отсутствие разграничения доступа к базе данных и файлам» можно реализовать угрозу :

а) Уязвимость конфиденциальности;

б) Уязвимость целостности;

в) **Все указанные уязвимости;**

г) Уязвимость доступности.

21) Что входит в методы защиты информации:

а) правовые методы защиты;

б) методы защиты от случайных угроз;

в) методы защиты от традиционного шпионажа и диверсий;

г) **все перечисленное, а еще организационные методы защиты, методы защиты от электромагнитных излучений и наводок, методы защиты от несанкционированного доступа, криптографические методы защиты и методы защиты от компьютерных вирусов.**

22. Не бывают аудита:

а) Внешнего;

б) Наружного;

в) Внутреннего;

г) Третьей стороной.

23. Для чего создается периметр безопасности?

а) Для создания системы СКУД

б) Для защиты участков, содержащих информацию и средства ее обработки

в) Для защиты всей контрольной зоны

г) Для защиты сейфа, в котором хранятся основные и резервные ключевые носители

д) Для защиты средств обработки информации

24. Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными, называется :

а) Оператором;

б) Хранителем;

в) Сервером;

г) Обработчиком.

25. СТО ВР ИББС-1.0 относится к :

а) Международным стандартам;

б) Национальным стандартам РФ;

в) Отраслевым стандартам РФ;

г) Ведомственным стандартам РФ.

Модуль 2. Организационная структура системы обеспечения безопасности автоматизированных систем.

1. Защита исполняемых файлов обеспечивается

а) обязательным контролем попытки запуска

б) криптографией

в) специальным режимом запуска

г) дополнительным хостом

2. Защита от форматирования жесткого диска со стороны пользователей обеспечивается

а) аппаратным модулем, устанавливаемым на системную шину ПК

б) системным программным обеспечением

в) специальным программным обеспечением

г) аппаратным модулем, устанавливаемым на контроллер

3. Из перечисленного ACL-список содержит:

а) срок действия маркера доступа;

б) домены, которым разрешен доступ к объекту;

в) операции, которые разрешены с каждым объектом;

г) тип доступа

4. Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются:

а) аутентификация;

б) идентификация;

в) целостность;

г) контроль доступа;

д) контроль трафика;

е) причастность

5. Из перечисленного в обязанности сотрудников группы информационной безопасности входят:

а) управление доступом пользователей к данным;

б) расследование причин нарушения защиты;

в) исправление ошибок в программном обеспечении;

д) устранение дефектов аппаратной части

6. Из перечисленного в ОС UNIX существуют администраторы:

а) системных утилит;

б) службы контроля;

в) службы аутентификации;

г) тиражирования;

д) печати;

е) аудита

7. Из перечисленного в файловых системах ОС UNIX права доступа к файлу определяются для:

а) владельца;

б) членов группы владельца;

в) конкретных заданных пользователей;

г) конкретных заданных групп пользователей;

д) всех основных пользователей

8. Из перечисленного для аутентификации по отпечаткам пальцев терминальных пользователей используются методы:

а) сравнение отдельных случайно выбранных фрагментов;
б) сравнение характерных деталей в графическом представлении;
в) непосредственное сравнение изображений;
г) сравнение характерных деталей в цифровом виде

9. Из перечисленного для разграничения доступа к файлу применяются флаги, разрешающие:
а) копирование;
б) чтение;
в) запись;
г) выполнение;
д) удаление

10. Из перечисленного доступ к объекту в многоуровневой модели может рассматриваться как:
а) чтение;
б) удаление;
в) копирование;
г) изменение

11. Из перечисленного контроль доступа используется на уровнях:
а) сетевом;
б) транспортном;
в) сеансовом;
г) канальном;
д) прикладном;
е) физическом

12. Из перечисленного методами защиты потока сообщений являются:
а) нумерация сообщений;
б) отметка времени;
в) использование случайных чисел;
г) нумерация блоков сообщений;
д) копирование потока сообщений

13. Из перечисленного на транспортном уровне рекомендуется применение услуг:
а) идентификации;
б) конфиденциальности;
в) контроля трафика;
г) контроля доступа;
д) целостности;
е) аутентификации

14. Из перечисленного подсистема управления криптографическими ключами структурно состоит из:
а) центра распределения ключей;
б) программно-аппаратных средств;
в) подсистемы генерации ключей;
г) подсистемы защиты ключей

15. В чем заключается метод защиты информации - разделение доступа (привилегий)?
а) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.
б) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.
в) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.

г) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.

д) В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

16. В чем заключается метод защиты информации - разграничение доступа?

а) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.

б) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.

в) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.

г) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.

д) В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

17. В чем заключается метод защиты информации - ограничение доступа?

а) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.

б) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.

в) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.

г) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.

д) В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

18. На чем основан принцип работы антивирусных мониторов?

а) На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю.

б) На проверке файлов, секторов и системной памяти и поиске в них известных и новых(неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски.

в) На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т. д.

г) На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные.

19. На чем основан принцип работы антивирусныхиммунизаторов?

а) На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные.

б) На проверке файлов, секторов и системной памяти и поиске в них известных и новых(неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски.

в) На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т. д.

г) На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю.

20. Что необходимо сделать при обнаружении файлового вируса?

а) Компьютер необходимо отключить от сети и проинформировать системного администратора.

б) Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются.

в) Вместо отключения компьютера от сети достаточно на период лечения убедиться втом, что соответствующий редактор неактивен.

21. Что необходимо сделать при обнаружении загрузочного вируса?

а) Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются.

б) Компьютер необходимо отключить от сети и проинформировать системного администратора.

в) Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен.

22. Что необходимо сделать при обнаружении макровируса?

а) Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен.

б) Компьютер необходимо отключить от сети и проинформировать системного администратора.

в) Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются.

23. В чем заключается принцип работы сетевого вируса?

а) Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

б) Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы;

в) Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.

г) Вирусы заражают файлы-документы и электронные таблицы популярных редакторов.

24. Источником каких угроз информации являются санкционированные программно-аппаратные средства?

а) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или

реструктуризацию носителей информации, удаление данных и т.п.); возникновение отказа в работе операционной системы.

б) стихийные бедствия; магнитные бури; радиоактивное излучение.

в) внедрение агентов в число персонала системы;вербовка персонала или отдельных пользователей, имеющих определенные полномочия; угроза несанкционированного копирования секретных данных пользователем; разглашение, передача или утрата атрибутов разграничения доступа.

г) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях); заражение компьютера вирусами с деструктивными функциями.

25. Какие угрозы информации относятся к искусственным?

а) ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков; структурные, алгоритмические и программные ошибки; действия человека, направленные на несанкционированные воздействия на информацию.

б) отказы и сбои аппаратуры; помехи на линиях связи от воздействий внешней среды; аварийные ситуации; стихийные бедствия.

в) аварийные ситуации; стихийные бедствия; ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков.

Модуль 3. Обеспечение безопасности АС.

1. Кто является основным ответственным за определение уровня классификации информации?

а) Руководитель среднего звена

б). Высшее руководство

в) Владелец

г) Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

а) Сотрудники

б) Хакеры

в) Атакующие

г) Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

в) Улучшить контроль за безопасностью этой информации

г) Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?

а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

б) Необходимый уровень доступности, целостности и конфиденциальности

в) Оценить уровень риска и отменить контрмеры

г) Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

а) Владельцы данных

б) Пользователи

в) Администраторы

г) Руководство

6. Что такое процедура?

а) Правила использования программного и аппаратного обеспечения в компании

б) Пошаговая инструкция по выполнению задачи

в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

г) Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

а) Поддержка высшего руководства

б) Эффективные защитные меры и методы их внедрения

в) Актуальные и адекватные политики и процедуры безопасности

г) Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

б) Когда риски не могут быть приняты во внимание по политическим соображениям

в) Когда необходимые защитные меры слишком сложны

г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?

а)Пошаговые инструкции по выполнению задач безопасности

б) Общие руководящие требования по достижению определенного уровня безопасности

в) **Широкие, высокоуровневые заявления руководства**

г) Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) Анализ рисков

б) **Анализ затрат / выгоды**

в) Результаты ALE

г) Выявление уязвимостей и угроз, являющихся причиной риска

11. Что лучше всего описывает цель расчета ALE?

а) Количественно оценить уровень безопасности среды

б) Оценить возможные потери для каждой контрмеры

в) Количественно оценить затраты / выгоды

г) **Оценить потенциальные потери от угрозы в год**

12. Тактическое планирование – это:

а) **Среднесрочное планирование**

б) Долгосрочное планирование

в) Ежедневное планирование

г) Планирование на 6 месяцев

13. Что является определением воздействия (exposure) на безопасность?

а) **Нечто, приводящее к ущербу от угрозы**

б) Любая потенциальная опасность для информации или систем

в) Любой недостаток или отсутствие информационной безопасности

г) Потенциальные потери от угрозы

14. Эффективная программа безопасности требует сбалансированного применения:

а) **Технических и нетехнических методов**

б) Контрмер и защитных механизмов

в) Физической безопасности и технических средств защиты

г) Процедур безопасности и шифрования

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

а) Внедрение управления механизмами безопасности

б) Классификацию данных после внедрения механизмов безопасности

в) **Уровень доверия, обеспечиваемый механизмом безопасности**

г) Соотношение затрат / выгод

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

а) Только военные имеют настоящую безопасность

б) Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности

в) Военным требуется больший уровень безопасности, т.к. их риски существенно выше

г) Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск?

а) Угрозы х Риски х Ценность актива

б) (Угрозы х Ценность актива х Уязвимости) х Риски

в) SLE х Частоту = ALE

г) **(Угрозы х Уязвимости х Ценность актива) х Недостаток контроля**

18. Что из перечисленного не является целью проведения анализа рисков?

а) **Делегирование полномочий**

б) Количественная оценка воздействия потенциальных угроз

в) Выявление рисков

г) Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

а) Поддержка

б) **Выполнение анализа рисков**

в) Определение цели и границ

г) Делегирование полномочий

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

а) Чтобы убедиться, что проводится справедливая оценка

б) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

в) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

г) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

21. Что является наилучшим описанием количественного анализа рисков?

а) Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности

б) Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков

в) Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков

г) Метод, основанный на суждениях и интуиции

22. Почему количественный анализ рисков в чистом виде не достижим?

а) Он достижим и используется

б) Он присваивает уровни критичности. Их сложно перевести в денежный вид.

в) Это связано с точностью количественных элементов

г) **Количественные измерения должны применяться к качественным элементам**

23. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

а) **Много информации нужно собрать и ввести в программу**

б) Руководство должно одобрить создание группы

в) Анализ рисков не может быть автоматизирован, что связано с самой природой оценки

г) Множество людей должно одобрить данные

24. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

а) Стандарты

б) Должный процесс (Dueprocess)

в) **Должная забота (Duecare)**

г) Снижение обязательств

25. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

а) Список стандартов, процедур и политик для разработки программы безопасности

б) Текущая версия ISO 17799

в) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях

г) Открытый стандарт, определяющий цели контроля

Модуль 4. Уязвимости АС.

1. Из каких четырех доменов состоит CobiT?

а) Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

б) Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

в) Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка

г) Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

2. Что представляет собой стандарт ISO/IEC 27799?

а) **Стандарт по защите персональных данных о здоровье**

б) Новая версия BS 17799

в) Определения для новой серии ISO 27000

г) Новая версия NIST 800-60

3. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

а) COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам

б) COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень

в) COSO учитывает корпоративную культуру и разработку политик

г) COSO – это система отказоустойчивости

4. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

а) NIST и OCTAVE являются корпоративными

б) **NIST и OCTAVE ориентирован на ИТ**

в) AS/NZS ориентирован на ИТ

г) NIST и AS/NZS являются корпоративными

5. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

а) Анализ связующего дерева

б) AS/NZS

в) NIST

г) **Анализ сбоев и дефектов**

6. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

а) Безопасная OECD

б) ISO\IEC

в) **OECD**

г) CPTED

7. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:

а) гаммирования;

б) подстановки;

в) **кодирования;**

г) перестановки;

д) аналитических преобразований.

8. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:

а)**гаммирования**

б) подстановки;

в) кодирования;

г) перестановки;

д) аналитических преобразований.

9. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

а)**гаммирования;**

б) подстановки;

в) кодирования;

г) перестановки;

д) аналитических преобразований.

10. Защита информации от утечки это деятельность по предотвращению:

а) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

б) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

в) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

г) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

д) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

11. Защита информации это:

а) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

б) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

в) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

г) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

д) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

12. Естественные угрозы безопасности информации вызваны:

а) деятельностью человека;

б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

в)) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

г) корыстными устремлениями злоумышленников;

д) ошибками при действиях персонала.

13. Икусственные угрозы безопасности информации вызваны:

а) деятельностью человека;

б) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

в) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

г) корыстными устремлениями злоумышленников;

д) ошибками при действиях персонала.

14. К основным непреднамеренным искусственным угрозам АСОИ относится:

а) физическое разрушение системы путем взрыва, поджога и т.п.;

б) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;

в) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

г) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

д) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

15. К посторонним лицам нарушителям информационной безопасности относится:

а) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;

б) персонал, обслуживающий технические средства;

в) технический персонал, обслуживающий здание;

г) пользователи;

д) сотрудники службы безопасности.

е) представители конкурирующих организаций.

ж) лица, нарушившие пропускной режим;

16. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

а) **черный пиар;**

б) фишинг;

в) нигерийские письма;

г) источник слухов;

д) пустые письма.

17. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

а) черный пиар;
б) фишинг;
в) нигерийские письма;
г) источник слухов;
д) пустые письма.

18. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:
а) **детектор;**
б) доктор;
в) сканер;
г) ревизор;
д) сторож.

19. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:
а)детектор;
б) **доктор;**
в) сканер;
г) ревизор;
д) сторож.

20. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:
а)детектор;
б) доктор;
в) сканер;
г) **ревизор;**
д) сторож.

21. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:
а)детектор;
б) доктор;
в) сканер;
г) ревизор;
д) **сторож.**

22. Активный перехват информации это перехват, который:
а) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
б) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
в) неправомерно использует технологические отходы информационного процесса;
г) осуществляется путем использования оптической техники;
д) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

23. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
а)активный перехват;
б) пассивный перехват;
в) **аудиоперехват;**
г) видеоперехват;
д) просмотр мусора.

24. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

а)активный перехват;
б) **пассивный перехват;**
в) аудиоперехват;
г) видеоперехват;
д) просмотр мусора.

25. Перехват, который осуществляется путем использования оптической техники называется:
а)активный перехват;
б) пассивный перехват;
в) аудиоперехват;
г) **видеоперехват;**
д) просмотр мусора.

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (25 вопросов в варианте)	Неправильный ответ / Правильный ответ	
Модуль 1		0,56
Модуль 2		0,56
Модуль 3		0,48
Модуль 4		0,4

Практические работы

Цель проведения практических работ – практическое освоение материала дисциплины.

Темы практических работ

Модуль 1. Общая характеристика информационной защиты автоматизированных систем.

1. Активы автоматизированных систем.
2. Инвентаризация активов автоматизированных систем.
3. Категорирование защищаемой информации.
4. Определение границ объекта информатизации, содержащего автоматизированную систему.
5. Классификация автоматизированных систем и требования по защите информации.
6. Классификация защищенности СВТ от НСД к информации.
7. Классы защиты межсетевых экранов.
8. Основные механизмы защиты автоматизированных систем.
9. Защита периметра компьютерных сетей и управление механизмами защиты.

Модуль 2. Организационная структура системы обеспечения безопасности автоматизированных систем.

10. Организационная структура системы обеспечения безопасности автоматизированных систем.
11. Институт ответственных за обеспечение информационной безопасности.
12. Регламентация действий пользователей и обслуживающего персонала автоматизированной системы.
13. Политика безопасности организации.
14. Распределение функций по обеспечению безопасности автоматизированных систем.
15. Организационно-распорядительные документы по обеспечению безопасности автоматизированных систем.
16. Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях.
17. Регламентация правил парольной и антивирусной защиты.

18. Регламентация порядка допуска к работе и изменения полномочий пользователей автоматизированной системы.

Модуль 3. Обеспечение безопасности АС.

19. Аппаратно-программные средства защиты информации от несанкционированного доступа.
20. Рекомендации по выбору средств защиты информации от несанкционированного доступа.
21. Обзор существующих на рынке средств защиты информации от несанкционированного доступа.
22. Способы аутентификации.

Модуль 4. Уязвимости АС.

23. Уязвимости АС и их классификация.
24. Угрозы, связанные с периметром корпоративной сети.
25. Обнаружение и устранение уязвимостей.
26. Возможности сканеров безопасности.

Практическая работа № 4

Модуль 1. Общая характеристика информационной защиты автоматизированных систем

Тема: Определение границ объекта информатизации, содержащего автоматизированную систему.

Цель: Отработка на практике методики построения защиты АС.

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

Аппаратура. Для выполнения лабораторной работы необходим персональный компьютер.

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

Критерии оценки практической работы

Структура работы	Критерии оценки	Распределение баллов
Одно практическое задание Модуль 1 Модуль 2 Модуль 3 Модуль 4	работа выполнена с ошибками и не получены ответы на все контрольные вопросы/ работа выполнена, но не получены ответы на все контрольные вопросы/ работа выполнена и получены ответы на все контрольные вопросы	 0/2/4 0/2/4 0/3/7 0/2/5

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

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

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

Дополнительная литература

1. Сердюк В.А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных систем предприятий. - М.: НИУ Высшая школа экономики, 2011. – 574 с. http://biblioclub.ru/index.php?page=book&id=74298&sr=1
2. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие. - М., Берлин: Директ-Медиа, 2015. – 253 с. http://biblioclub.ru/index.php?page=book&id=276557&sr=1
3. Анисимов А.А. Менеджмент в сфере информационной безопасности: Учебное пособие. - М.: Интернет-Университет Информационных Технологий, 2009. – 176 с. http://biblioclub.ru/index.php?page=book&id=232981&sr=1
4. Мельников В.П., Клейменов С.А., Петраков А.М.Информационная безопасность и защита информации: Учебное пособие. – М.: Академия. – 2011 с. https://bashedu.bibliotech.ru/Reader/Book/2013080217381731971500009579

5.2. 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 «Университетская библиотека онлайн» - https://biblioclub.ru
2. Электронная библиотечная система «ЭБ БашГУ» - https://elib.bashedu.ru
3. Электронная библиотечная система БашГУ – www.bashlib.ru
4. Электронная библиотечная система издательства «Лань» - https://e.lanbook.com
5. Антиплагиат.ВУЗ. Договор № 81 от 27.04.2018 г. Срок действия лицензии до 04.05.2019 г., договор № 1104 от 18.04.2019 г. Срок действия лицензии до 04.05.2020 г
6. Банк нормативно-правовых актов РФ Министерства юстиции РФ - http://zakon.scli.ru/ru/legal_texts/index.php
7. Справочная правовая система Консультант Плюс. Договор №31705775411 от 07.12.2017 г. http://www.consultant-plus.ru
8. Национальные стандарты РФ в области информационной безопасности: http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii
9. Нормативные документы и материалы сайта ФСТЭК России (Федеральной службы по техническому и экспортному контролю России): https://fstec.ru/ Раздел «Национальные старты информационной безопасности» (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty)

Государственные информационно-правовые системы:

1. Научный центр правовой информации при министерстве Юстиций РФ - http://www.scli.ru
2. Официальный интернет-портал правовой информации - http://pravo.gov.ru
3. Информационно-правовая система «Законодательство России» - http://pravo.fso.gov.ru
4. Модуль «Документы - Президент России» - http://www.kremlin.ru/acts
5. Банк документов, подписанных Президентом России - http://kremlin.ru/acts/bank
6. База данных «Федеральные законы» - http://graph.garant.ru:8080/SESSION/PILOT/main.htm
7. Автоматизированная система обеспечения законодательной деятельности государственной думы (законопроекты и законодательные инициативы) - http://asozd.duma.gov.ru/
8. База данных «Издания по общественным и гуманитарным наукам» (на платформе

EastView) - Ссылка http://www.ebiblioteka.ru(вход из сети вуза без регистрации).

9. Банк данных "Библиотека копий официальных публикаций правовых актов» при ассоциации юристов России - http://alrf.consultant.ru/
10. Банк данных "Копии правовых актов: Российская Федерация» - http://giod.consultant.ru/
11. Банк данных "Нормативно-правовые акты Федерального Собрания Российской Федерации - http://duma.consultant.ru/

Другие профессиональные базы данных и информационно-справочные системы:

1. Электронная база данных диссертаций РГБ (авторизованный доступ по паролю в сети вуза) – Ссылка: http://dvs.rsl.ru
2. База данных «Вестники Московского университета» (на платформе EastView) (вход без регистрации). - Ссылка http://www.ebiblioteka.ru/browse/udb/12.
3. AnnualReviews – обзор журналов по общественно-научной тематике и др. – доступ из сети вуза. – Ссылка: http://www.annualreviews.org/
4. Computers & Applied Sciences Complete (EBSCO) - доступвсетивуза, языканглийский. - Ссылка: http://search.ebscohost.com/
5. SCOPUS - наукометрическая, библиографическая и реферативная база данных издательской корпорации Elsevier. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://www.scopus.com/
6. TaylorandFrancis – База полнотекстовых научных журналов, книг. Язык английский. – доступ из сети вуза. – Ссылка: http://www.tandf
7. WebofScience - наукометрическая, библиографическая и реферативная база данных издательской корпорации ThomsonReuters. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://apps.webofknowledge.com/
8. Wiley - Полнотекстовая база данных статей из 1400 журналов издательства Wiley по всем отраслям знаний. Язык английский. Доступ из сети вуза без регистрации. – Ссылка: http://onlinelibrary.wiley.com/
9. Сайт по информационной безопасности: http://securitypolicy.ru/; его раздел: «Документы, стандарты и методики по информационной безопасности»: http://securitypolicy.ru/
10. Докипедия: http://dokipedia.ru
11. Словари и энциклопедии On-Line- http://www.dic.academic.ru

Программноеобеспечение

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 № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2.** ***учебная аудитория для проведения лабораторных работ*****:** Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (гуманитарный корпус). **3.** ***учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608	Лекции, лабораторные и практические занятия, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный ClassicNorma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный LumienMasterPikture 153*203 MatteWhiteFiberClas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSizeIcon 600-камера, интер-ая система со встроенным короткофокусным проектором PrometheanActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Thermaltake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование:

(гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **4.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **5.** ***учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **6.** ***помещения для***		проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технические средства обработки информации, стенд "Устройство ПК". **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.

самостоятельной работы: читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **7*. помещение для хранения и профилактического обслуживания учебного оборудования:*** аудитория № 523 (гуманитарный корпус).		

Приложение № 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Информационная безопасность автоматизированных систем** на 7 семестр
___очная_ф/о___

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	54,2
лекций	18
практических/ семинарских	36
лабораторных	–
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на самостоятельную работу обучающихся (СР)	89,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к зачету (Контроль)	–

Форма контроля
Зачет 7 семестр

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Информационная безопасность автоматизированных систем** на 8 семестр
очная ф/о

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	49,2
лекций	16
практических/ семинарских	32
лабораторных	–
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на самостоятельную работу обучающихся (СР)	31,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к экзамену (Контроль)	27

Форма контроля
Экзамен 8 семестр

Семестр 7

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / СЕМ	ЛР	СР		
1	2	3	4	5	6	8	9
1	Модуль 1. Общая характеристика информационной защиты автоматизированных систем. Тема: Особенности современных автоматизированных систем как объектов защиты. Тема: Основные механизмы защиты автоматизированных систем. Тема: Применение штатных и дополнительных средств защиты информации от несанкционированного доступа. Тема: Назначение и возможности средств защиты информации от несанкционированного доступа. Тема: Рекомендации по выбору средств защиты информации от несанкционированного доступа.	2 2 2 2 2	4 4 4 4 4		10 10 10 10 10	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, тест
2	Модуль 2. Организационная структура системы обеспечения безопасности автоматизированных систем. Тема: Технология управления безопасностью информации и ресурсов в автоматизированной системе. Тема: Институт ответственных за обеспечение	2 2	4 4		10 10	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, тест

	информационной безопасности. Тема: 3Политика безопасности организации. Тема: Мероприятия по созданию и обеспечению функционирования комплексной системы защиты.	 2 2	 4 4		 10 9,8		
Всего часов		18	36	0	89,8		

Семестр 8

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / СЕМ	ЛР	СР		
1	2	3	4	5	6	8	9
1	Модуль 3. Обеспечение безопасности АС. Тема: Проблемы обеспечения безопасности в АС. Тема: Типовая корпоративная сеть. Тема: Средства защиты сетей. Тема: Защита периметра корпоративной сети.	 2 2 2 2	 4 4 4 4		 4 4 4 4	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, тест
2	Модуль 4. Уязвимости АС. Тема: Обнаружение и устранение уязвимостей. Тема: Мониторинг событий безопасности Введение в управление журналами событий. Тема: Средства анализа защищенности АС. Тема: Введение в технологию обнаружения атак.	 2 2 2 2	 4 4 4 4		 4 4 4 3,2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы …	практическая работа, тест
		16	32	0	31,8		
Всего часов		34	68	0	121,6		