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

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

Зав. кафедрой _____ /Исмагилова А.С.

Согласовано:
Председатель УМК института

_____/Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина
Защищенные автоматизированные системы

Часть, формируемая участниками образовательных отношений

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации
(в системе государственного и муниципального управления)

Квалификация
бакалавр

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

_____ / Миронова Н.Г.

Для приема: 2021 г.

Уфа 2021 г.

Составитель: к.филос.н. Мироноваа Наталия Геннадьевна

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

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

Заведующий кафедрой / Исмагилова А.С. /

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

Заведующий кафедрой _____/ Исмагилова А.С. /

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 результатами освоения образовательной программы 4

2. Цель и место дисциплины в структуре образовательной программы 4

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 7

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 19

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**
экспериментально-исследовательский	ПК-4. Способен проводить контроль защищенности информации	4.1. Знает методы контроля защищенности информации, каналы утечки информации, нормативно-правовую базу защиты информации	Знать защищенности информации, каналы утечки информации, нормативно-правовую базу защиты информации в части обеспечения работы защищенных АС; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования к разработке и эксплуатации АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС; технологии и способы обеспечения защиты ИС/АС.
		ПК-4.2. Умеет применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации	Уметь применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации в части обеспечения работы защищенных АС; уметь использовать средства и технологии защиты в ИС при решении профессиональных задач
		ПК- 4.3. Владеет навыками применения методов контроля защищенности информации, определения каналов утечки информации, применения нормативно-правовой базы защиты информации.	Владеть навыками применения методов контроля защищенности информации, определения каналов утечки информации, применения нормативно-правовой базы защиты информации в части обеспечения работы защищенных АС; владеть навыками управления защитой информации в ИС/АС.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Защищенные автоматизированные системы» относится к части, формируемой участниками образовательных отношений.

Дисциплина изучается на 4 курсе бакалавриата в 7 и 8 семест*рах.*

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

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении № 1.

4. Фонд оценочных средств по дисциплине

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

ПК-4. Способен проводить контроль защищенности информации

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
4.1. Знает методы контроля защищенности информации, каналы утечки информации, нормативно-правовую базу защиты информации	Знать защищенности информации, каналы утечки информации, нормативно-правовую базу защиты информации в части обеспечения работы защищенных АС; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования к разработке и экс-	Не знает	Слабо знает указанные требования и технологии.	Демонстрирует хорошее знание указанных требований и технологий, но не всегда способен увязать их с практикой управления службой защиты информации.	Демонстрирует целостные, системные знания в указанной сфере.

	плуатации АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС; технологии и способы обеспечения защиты ИС/АС.				
ПК-4.2. Умеет применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации	Уметь применять методы контроля защищенности информации, определять каналы утечки информации, применять нормативно-правовую базу защиты информации в части обеспечения работы защищенных АС; уметь использовать средства и технологии защиты в ИС при решении профессиональных задач	Не умеет	Слабо демонстрирует указанные умения и знания, без связи навыками решения задач организации службы защиты информации.	Демонстрирует хорошее теоретическое знание компетенции, но недостаточное владение практической стороной при решении задач организации службы защиты информации	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации
ПК- 4.3. Владеет навыками применения методов контроля защищенности информации, определения каналов утечки информации, применения нормативно-правовой базы защиты информации.	Владеть навыками применения методов контроля защищенности информации, определения каналов утечки информации, применения нормативно-правовой базы защиты информации в части обеспечения работы защищенных АС; владеть	Не владеет	Слабо демонстрирует указанные навыки.	Демонстрирует хорошее владение компетенцией, но имеет устаревшие и малоактуальные сведения.	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации службы защиты информации.

	навыками управления защитой информации в ИС/АС.				

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-4. Способен проводить контроль защищенности информации

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ПК-4.7 знает режимы и особенности работы средств и систем обработки и передачи информации	Знать режимы и особенности работы средств и систем обработки и передачи информации в части обеспечения работы защищенных АС; требования стандартов, законов, регуляторов к уровню защищенности автоматизированных систем с учетом классов защищенности; требования к разработке и эксплуатации АС в защищенном исполнении; знает угрозы и уязвимости ИС/АС; технологии и способы обеспечения защиты ИС/АС.	практические задания; опрос/доклад; отчет по практикам); компьютерный тест
ПК-4.8 умеет использовать знания о режимах и особенностях работы средств и систем обработки и передачи информации	Уметь использовать знания о режимах и особенностях работы средств и систем обработки и передачи информации в части обеспечения работы защищенных АС; уметь использовать средства и технологии защиты в ИС при решении профессиональных задач	практические задания; опрос/доклад; отчет по практикам); компьютерный тест
ПК-4.6 Владеет навыками анализа и выбора режимов работы программно-аппаратных средств защиты информации в компьютерных сетях.	Владеть навыками анализа и выбора режимов работы программно-аппаратных средств защиты информации в компьютерных сетях, в части обеспечения работы защищенных АС; владеть навыками управления защитой информации в ИС/АС. .	практические задания; опрос/доклад; отчет по практикам); компьютерный тест

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

Для зачета (в 7 семестре): текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания для зачета:

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

не зачтено – от 0 до 59 рейтинговых баллов).

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

Для экзамена (в 8 семестре): текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10;

Шкалы оценивания для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

Рейтинг – план дисциплины
«Защищенные автоматизированные системы»

Направление подготовки 10.03.01 Информационная безопасность

курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль (Раздел) 1				
Текущий контроль				
Аудиторная работа				
1. Доклады/ практические задания	**5**	**3**	**0**	15
2. Устный опрос	**2,5**	**1**	**0**	4
Рубежный контроль				
1. Отчет по практическим работам	**5**	**2**	**0**	10
Модуль (Раздел) 2				
Текущий контроль				
Аудиторная работа				
1. Доклады/ практические задания	**5**	**6**	**0**	30
2. Устный опрос	**2,5**	**1**	**0**	4
Рубежный контроль				
1. Отчет по практическим работам	**5**	**4**	**0**	20
2. Тест итоговый (зачетный)	**1**	**20**	**0**	20
Поощрительные баллы				
1. Студенческая олимпиада				5
2. Публикация статей				5
3. Работа со школьниками (кружок, конкурсы, олимпиады)				
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			**0**	**–6**
2. Посещение практических (семинарских, лабораторных) занятий			**0**	**–10**
Итоговый контроль				
Зачет				

Рейтинг – план дисциплины
«Защищенные автоматизированные системы»

Направление подготовки 10.03.01 Информационная безопасность

курс 4, семестр 8

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль (Раздел) 3				
Текущий контроль				**11**
Аудиторная работа				
1. Доклады	**4**	**4**	**0**	16
Рубежный контроль				**1**
1. Устный опрос	**2**	**2**	**0**	4
Модуль (Раздел) 4				
Текущий контроль				**14**
Аудиторная работа				
1. Практические задания	**4**	**6**	**0**	24
Рубежный контроль				**5**
1. Устный опрос	**2**	**3**	**0**	6
2. Тест итоговый	**1**	**20**	**0**	20
Поощрительные баллы				
1. Студенческая олимпиада				**0**
2. Публикация статей				**10**
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			**0**	**–6**
2. Посещение практических (семинарских, лабораторных) занятий			**0**	**–10**
Итоговый контроль				
Экзамен				**30**

Экзаменационные билеты

Структура экзаменационного билета:

Экзаменационный билет содержит 2 теоретических вопроса из нижеприведенного перечня.

Перечень вопросов для экзамена:

1. Угрозы и риски информационной безопасности, связанные с использованием информационных систем.
2. Понятие защищенной информационной системы. Области применения защищенных ИС.
3. Примеры отечественных защищенных ИС.
4. Хранения данных при реализации ЗИС. СУБД для организации защищенных ИС.
5. ОС в защищенном исполнении.
6. Средства и способы программной реализации защиты информации.
7. Методологии проектирования ИС. Принципы проектирования и разработки ЗИС.
8. Этапы проектирования ЗИС.
9. Возможные уязвимости информационной безопасности для ИС и меры по их снижению, реализуемые на этапе разработки ИС.
10. Требования нормативных документов ФСТЭК, ФСБ и др. отечественных регуляторов к уровню защищенности информационных систем различных классов.
11. Классификация информационных систем. Интеграция приложений и информационных систем.
12. Роль специалиста по информационной безопасности в разработке, модернизации, внедрении ИС, в т.ч. защищенных ИС.
13. Этапы разработки информационных систем. Язык нотаций UML и виды диаграмм и моделей, используемые для проектирования ИС
14. Понятие логической модели предметной области в рамках CASE-технологии и основные виды и последовательность работ, рекомендуемые при построении этих моделей.
15. Методологии моделирования предметной области, информационных процессов (idef0, dfd, idef3, bpmn и др.). Методология функционального моделирования SADT.
16. Средства и языки нотаций для описания деловых процессов. BPMN.
17. Задачи обеспечения ИБ, угрозы ИБ, предпосылки уязвимости ИС.
18. Требования к уровню защищенности ИС и обрабатываемой в них информации, в зависимости от уровня конфиденциальности и критичности информации.
19. Меры и подходы к обеспечению защищенности ИС на этапах разработки
20. Проектирование СЗИ для ИС (этапы). Технические средства защиты информации в ИС.
21. ГИС и требования ФСТЭК и ФСБ к их уровню защищенности
22. ИСПДн и требования ФСТЭК и ФСБ к их уровню защищенности
23. АИС, АСУ и требования ФСТЭК и ФСБ к их уровню защищенности
24. ИС реального времени и требования к надежности таких ИС.

Образец экзаменационного билета:

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

Направление подготовки 10.03.01 «Информационная безопасность»

Дисциплина: Защищенные автоматизированные системы

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 20

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

Зав. кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии оценки (в баллах):

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

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

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

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

Планы семинарских занятий

Раздел 1. Требования безопасности информационных систем в защищенном исполнении

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

Цель: знакомство с теоретическими представлениями об информационных процессах.

Содержание: доклады на темы из списка:

Доклады:

1. Информационные системы. Классы ИС/АСУ.
2. Виды и свойства информации. Угрозы информационной безопасности, реализуемые с применением ИС.
3. Представление о защищенных ИС (определение, виды, требования к ЗИС, связанные с защищенностью).
4. Области использования открытых ИС. Отличие ЗИС от ОИС.
5. Применение защищенных ИС (цели, задачи обеспечения ИБ объектов; области применения ЗИС (медицина, госуправление, правоохранительные органы/МВД); примеры.
6. Проблемы информационной безопасности при использовании ИС, АИС, АСУ

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

Содержание: доклады на темы из списка:

1. Источники, способы и результаты дестабилизирующего воздействия на информацию; Их

выявление и оценка (общий алгоритм и особенности).
2. Методы и средства защиты информационных систем.
3. Проблема оценки защищенности информационных систем среды.
4. Программные закладки и методы противодействия.
5. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies.
6. Международные стандарты, ГОСТы и нормативные документы, определяющие требования к ИС/АС. Уровни защищенности и классы ИС. Требования к уровню защищенности автоматизированных систем с учетом класса защищенности. Угрозы ИБ, предпосылки уязвимости ИС.
7. ITSEC, «Оранжевая книга», ITIL, отечественные стандарты защищенности – о требованиях к ИС.
8. Требования к защищенности ИС с учетом обрабатываемой в них информации, масштаба, функционального назначения.
9. Нормативные и методические документы регуляторов (ФСТЭК, ФСБ) - про ЗИС («Меры защиты информации в ГИС» и проч.)
10. ИС/АС в защищенном исполнении – примеры, характеристики, функционал, безопасность.

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

Содержание: (темы для обсуждения, докладов, исследования)

1. Средства описания и моделирования деловых процессов, информационных процессов.
2. Этапы разработки информационных систем
3. Уровни представления предметной области при проектировании информационной системы.
4. Составление задания на разработку ИС – методологические аспекты.
5. Проектирование ЗИС. Анализ и определение требований к уровню защищенности ПС/ИС
6. Способы хранения информации.
7. Интеграция приложений и информационных систем.

Раздел 2. Представление о разработке информационных систем в защищенном исполнении

Практическое занятие №. 4. Теоретические основы построения защищённых автоматизированных систем (2 часа)

Содержание: (темы для обсуждения, докладов, исследования)

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

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

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

Содержание: (темы для обсуждения, докладов, исследования)

Подходы к созданию защищённых систем.
Проблемы проектирования и реализации защищенных систем.
Методика определения состава защищаемой информации.

Этапы работы по выявлению состава защищаемой информации.
Требования к содержанию документов по общесистемным решениям.
Ведомость проекта. Пояснительная записка к проекту.

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

Содержание: (темы для обсуждения, докладов, исследования)

1. Роль специалиста по информационной безопасности в разработке, модернизации, внедрении ИС, в т.ч. защищенных ИС.
2. Стандарты проектирования систем защиты информации
3. Классификация угроз безопасности. Этапы создания модели угроз
4. Классификации уязвимостей системы
5. Модель нарушителя
6. Классификация нарушителей в соответствии с документами регуляторов.
7. Защита каналов утечки. Мониторинг (аудит) действий пользователей. Классификация внутренних нарушителей
8. Нетехнические меры защиты от внутренних угроз.
9. Криптографическая защита информации. Требования к шифрованию.
10. Требования к аутентификации в ИС. Аутентификация по IP-адресу.

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

Содержание: (темы для обсуждения, докладов, исследования)

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

Практические занятия № 8, 9. Особенности построения систем защиты ИС (ЗИС) (4 часа)

Содержание: (темы для обсуждения, докладов, исследования)

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

Тестирование (зачетное)

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

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

Раздел 3. Показатели качества и надежности ИС. Сертификация ИС

Практическое занятие № 10, 11. Показатели качества и надежности ЗИС. Аудит защищённой ИС (4 часа)

Содержание: (темы для обсуждения, докладов, исследования)

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

Устный опрос по теме занятий

Практическое занятие № 12, 13. Обзор ЗИС и технологий обеспечения безопасности работы ИС (примеры, характеристики ЗИС, области применения ЗИС, встроенные средства безопасности, возможности ЗИС) (4 часа)

Содержание: (темы для обсуждения/практической реализации/ исследования)

Устный опрос по теме занятия

1. Основные направления защиты. Защита документов. Защита каналов утечки.
2. Мониторинг (аудит) действий пользователей.
3. Технические и программные средства аудита/контроля. Классификация внутренних нарушителей.
4. Сетевые фильтры – назначение, виды. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Технологии firewall. Политика безопасности firewall'a.
5. Системы анализа и оценки уязвимостей. Процесс анализа уязвимостей. Классификация инструментальных средств анализа уязвимостей. Возможности и недостатки систем анализа уязвимостей.
6. Цели и задачи использования IDS. Возможности IDS. Стратегия развертывания IDS. Типы атак, определяемых IDS.
7. Безопасность DNS. Сервисы DNS. Инфраструктура DNS. Компоненты DNS и понятие безопасности для них. Основные механизмы безопасности для сервисов DNS. Данные DNS и ПО DNS. Зонный файл. Name-серверы. Авторитетные name-серверы. Кэширующие

name-серверы. Resolver'bi. Транзакции DNS. Запрос / ответ DNS. Безопасность окружения DNS. Угрозы и обеспечение защиты платформы хоста. Угрозы ПО DNS. Угрозы для данных DNS.

8. Управление ресурсами на уровне ОС. Альтернативные платформы для web-сервера. Trusted ОС. Тестирование безопасности операционной системы. Действия для обеспечения безопасности ОС, на которой выполняется web-сервер.
9. Уязвимости технологий активного содержимого на стороне клиента. Уязвимости технологий создания содержимого на стороне сервера. Список действий для обеспечения безопасности web-содержимого.
10. Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе.

Раздел 4. Эксплуатация ЗИС

Практическое занятие № 14-16 Технологии, механизмы и способы обеспечения безопасности в защищенной ИС (с учетом разных факторов). (6 часов)

Содержание: (задания для исследования, доклады)

1. Базовые элементы и устройства обеспечения сетевой безопасности ИС. Компоненты инфраструктуры ИС.
2. Практика использования конкретной ИС/ЗИС. Знакомство с интерфейсом, функционалом, встроенными средствами безопасности и т.д.
3. Устный опрос.
4. Подготовка аналитического отчета по результатам освоения ЗИС.

Практическое занятие № 17-18. Администрирование и эксплуатация защищенной ИС/АС. Управление рисками и инцидентами управления безопасностью (4 часа)

Содержание: (задания для исследования, доклады)

1. Средства обеспечения отказоустойчивости автоматизированной системы
2. Порядок выполнения обязанностей администратора автоматизированной системы
3. Эксплуатационная документация защищенной автоматизированной системы
4. Нетехнические меры защиты от внутренних угроз

Практическое занятие № 19. Технические средства защиты информации в ИС (2 часа)

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

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

Опрос по результатам освоения материалов и практической работы.

Практическое занятие № 20. Итоговое тестирование (тест №2) (2 часа)

Тест компьютерный.

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

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

Типовые тестовые задания

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

Тестирование выполняется в виде компьютерного тестирования в СДО и личном кабинете студента (2 теста - по результатам 7 и 8 семестров).

Пример тестовых вопросов:

1. Верно ли утверждение, что информация обладает следующими свойствами, отражающими ее природу и особенности использования: кумулятивность, эмерджентность, неассоциативность, и старение информации.

1) Верное утверждение;
2) Не верное утверждение.

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

3. Деление информационных систем на одиночные, групповые, корпоративные, называется классификацией

1) По масштабу;
2) По сфере применения;
3) По способу организации.

4. Системы обработки транзакций по оперативности обработки данных разделяются на пакетные информационные системы и _____ информационные системы. *(вставьте правильное)*

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

Критерии оценки результатов 2-х тестирований (в баллах)*:*

-1 баллов выставляется студенту за каждый тестовый вопрос, если ответ на вопрос теста дан верно;

-0 баллов выставляется студенту за каждый тестовый вопрос, если ответ на вопрос теста дан ошибочный;

Тест № 1 по результату освоения разделов 1 и 2 (7 семестр) состоит из 20 вопросов и оценивается в совокупности до 20 баллов.

Тест № 2 по результату освоения разделов 3,4 (8 семестр) состоит из 20 вопросов и оценивается в совокупности до 20 баллов.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

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

Дополнительная литература:

4. Аверченков В.И., Лозбинев Ф.Ю., Тищенко А.А.Информационные системы в производстве и экономике: учебное пособие. - М.: Флинта, 2011. – 274 с. - http://biblioclub.ru/index.php?page=book&id=93265&sr=1
5. Алдохина О.И., Басалаева О.Г.Информационно-аналитические системы и сети: учебное пособие, Ч. 1. Информационно-аналитические системы: Учебное пособие. - Кемерово: КемГУКИ, 2010. – 148 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=227684&sr=1
6. Блинков Ю.В. Основы теории информационных процессов и систем: учебное пособие. - Пенза. Пензенский государственный университет архитектуры и строительства. – 2011, 184 с. – Режим доступа: http://window.edu.ru/resource/055/78055/files/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D1%8B_%D1%82%D0%B5%D0%BE%D1%80%D0%B8%D0%B8_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC_%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81%D0%BE%D0%B2.pdf
7. Бураков П.В., Петров В.Ю. Информационные системы в экономике: Учебное пособие. - СПб.: СПбГУ ИТМО, 2010. - 66 с. - http://window.edu.ru/resource/399/67399/files/itmo436.pdf
8. Бурцева Е.В., Рак И.П., Селезнев А.В., Терехов А.В., Чернышов В.Н. Информационные системы: Учебное пособие. - Тамбов: Изд-во ТГТУ, 2009. - 128 с. - http://window.edu.ru/resource/260/68260/files/Terehov_c.pdf
9. Володин Д.О., Матчин В.Т., Минаков В.И., Мордвинов В.А., Романов Д.Д., Третьяков А.А., Шленов А.Ю. и др. Моделирование информационных процессов и систем. - М.: МГДД(Ю)Т, МИРЭА, ГНИИ ИТТ "Информика", 2002. - 50 с. - http://window.edu.ru/resource/015/47015/files/mirea015.pdf
10. Гарифуллина С.Р. Система управления базами данных: Учебное пособие для студентов и магистрантов естественнонаучных и гуманитарных факультетов университета.. – Уфа: РИЦБашГУ, 2012. – 80 с. -

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

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

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

Программное обеспечение

1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Up-

grade 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. 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
Аудитория: 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).	Лекции	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двухполосный 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 APAPT MA1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт APAPT MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-

		связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.
Лаборатория компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).	Практические занятия	**Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Программное обеспечение** 1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle). GNU General Public License.
Компьютерный класс 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 компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).	Практические занятия (семинары)	**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 Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференцсвязи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром**.** **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноут-

		бук 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. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Программное обеспечение** 1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle). GNU General Public License.

Приложение № 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Защищенные автоматизированные системы
на _7_ семестр
очная форма обучения

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (з.е. / часов)	3/108
Учебных часов на контактную работу с преподавателем:	36,2
лекций	18
практических/ семинарских	18
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)	71,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	
Учебных часов на подготовку к экзамену	0

Форма контроля:
Зачет 7 семестр

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины «Защищенные автоматизированные системы»
на 8 семестр
очная форма обучения

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (з.е. / часов)	3/108
Учебных часов на контактную работу с преподавателем:	45,2
лекций	22
практических/ семинарских	22
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)	35,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	
Учебных часов на подготовку к экзамену (Контроль)	27

Формы контроля:
Экзамен 8 семестр

№ п/п	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР/СЕМ	ЛР	СР		
1	2	3	4	5	6	7	8
Раздел 1. Требования безопасности информационных систем в защищенном исполнении							
1.	1.1. Виды и категории программных систем. Категории ИС с повышенными требованиями к защищенности. **Содержание**: Открытые и защищенные ИС. Средства защиты открытых информационных систем. Виды и примеры защищенных ИС (ГИС/ГАС/ИСПДн/АИС/АС и т.д.) Концепция «защищенные информационные системы»; модель защищенности ИС. Методология анализа защищенности информационной системы	2	2		2	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос;
2.	1.2. Международные стандарты, ГОСТы и нормативные документы, определяющие требования к ИС/АС. Уровни защищенности и классы ИС. Требования к уровню защищенности автоматизированных систем с учетом класса защищенности. Угрозы ИБ, предпосылки уязвимости ИС. **Содержание**: ITSEC, «Оранжевая книга», ITIL, отечественные стандарты защищенности – о требованиях к ИС. Тре-	2	2		6	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос;

	бования к защищенности ИС с учетом обрабатываемой в них информации, масштаба, функционального назначения и т.д. Нормативные и методические документы регуляторов (ФСТЭК, ФСБ) про ЗИС («Меры защиты информации в ГИС» и проч.)						
3	1.3. Анализ и оценка информационных рисков, угроз и уязвимостей при разработке/эксплуатации защищенной системы обработки информации; класс (уровень) защищенности ИС; угрозы безопасности информации применительно к процессам функционирования ИС. **Содержание**: объекты уязвимости; угрозы. Уязвимости архитектуры клиент-сервер (ОС, рабочих станций и серверов, СУБД, каналов связи и сетевого оборудования). Уязвимость системных утилит, команд и сетевых сервисов на примере стека протоколов tcp/ip (Telnet, FTP, NFS, DNS, NIS, World Wide Web, команды удаленного выполнения, Sendmail и электронная почта, другие утилиты). Средства замены уязвимых сервисов TCP/IP. Уязвимости технологий программирования, «человеческий фактор» (ошибки разработки); классификация внутренних нарушителей на этапе эксплуатации ИС. Анализ и оценка информационных рисков, угроз и уязвимостей при разработке/эксплуатации защищенной системы обработки информации; класс (уровень) защищенности ИС; Сервисы безопасно-	2	2		8	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос;

	сти. Средства обеспечения ИБ в сетях. Их назначение, особенности применения и примеры.						
Раздел 2. Представление о разработке информационных систем в защищенном исполнении							
4	2.1. Требования международных, национальных и отраслевых стандартов к разработке ПО к безопасности защищенных ИС (на этапах разработки и эксплуатации ИС/АС в защищенном исполнении). **Содержание**: Комплексный и фрагментарный подходы к защите ИС. Эшелонированная защита. Четырехуровневая модель открытой системы. Руководящие документы и стандарты по защите открытых сетей. Топология сети: физическая изоляция; изоляция протокола; выделенные каналы. Требования к архитектуре информационных систем для обеспечения безопасности. Требования международных, национальных и отраслевых стандартов к разработке ПО к безопасности защищенных ИС (на этапах разработки и эксплуатации ИС/АС в защищенном исполнении).	2	2		8	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос;
5	2.2. Этапы жизненного цикла ИС (в т.ч. специфика разработки и эксплуатации ЗИС). CASE-средства проектирования ИС. **Содержание**: Этапы построения системы безопасности ИС. Разработка требований к ЗИС, концепции ЗИС; техзадание, проектирование, разработка, документировние, аттестация ЗИС. Содержание ат-	2	2		8	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос;

	тестационного испытания (для ЗИС). Оценка защищенности ИС/АС. Эксплуатация ЗИС на объекте защиты. Аудит безопасности (обследование) существующей системы защиты ИС, анализ рисков, формирование требований и выработка первоочередных мер защиты,. Обзор средств для выполнения обследования и проектирования ИС в з.и.						
6	2.3. Языки, среды и средства разработки ИС в защищенном исполнении. Проблемы безопасности, обусловленные технологиями и подходами к разработке ПС. **Содержание**: обзор средств проектирования и разработки защищенных ИС. Технологии и принципы разработки защищенных ИС, Проблемы безопасности, обусловленные технологиями и подходами к разработке ПС.	2	2		10	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос;
7	2.4 Показатели надёжности и отказоустойчивости ПО/ИС; средства обеспечения надёжности ПО (резервирование, введение структурной избыточности, протоколирование; модели надёжности программ; алгоритмы автоматического восстановления ИС и т.д.). **Содержание**: Оценка уровня защищенности ИС (по цели, средству и исполнению). Показатели надёжности и отказоустойчивости ПО/ИС; средства обеспечения надёжности ПО (резервирование, введение структурной избыточности, протоколирование; модели надёжности программ; алгоритмы автоматического вос-	2	2		8	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос;

	становления ИС и т.д.).						
8	2.5. Принципы и особенности разработки систем в защищенном исполнении. Проектная, техническая, рабочая, пользовательская документация на ИС. **Содержание**: Стандартизация подходов к обеспечению информационной безопасности; комплексная (интегральная) безопасность ИС Проблемы (в т.ч. методологические) создания ЗИС.	2	2		10	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос/доклад; тест
9	2.6. Базы данных и информационные системы. О технологиях безопасного хранения и обработки данных в ИС. Особенности организации данных в различных моделях данных. **Содержание**: обеспечение безопасности данных для ЗИС; технологии/модели данных и средств безопасного хранения данных в ИС.	2	2		11,8	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос/доклад; тест
	Итого за 7 семестр:	***18***	***18***	***18***	***71,8***		
Раздел 3. Показатели качества и надежности ИС. Сертификация ИС							
10	3.1. Показатели качества и надежности ИС в защищенном исполнении. Средства безопасности, реализуемые в ЗИС. Аттестация ЗИС	4	4		6	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос;
11	3.2. Обзор ЗИС (примеры, характеристики ЗИС, области применения ЗИС, встроенные средства безопасности, возможности ЗИС).	4	4		6	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос;
Раздел 4. Эксплуатация ЗИС.							
12	4.1. Технологии, механизмы и способы обеспечения безопасности в защищенной	6	6		8	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос/доклад; тест

	ИС (с учетом разных факторов). Содержание: Базовые элементы и устройства обеспечения сетевой безопасности ИС. Компоненты инфраструктуры ИС.						
13	4.2. Администрирование информационных систем. Доступ к данным безопасности. Монитор безопасности, протоколирование, аудит, шифрование, контроль целостности данных, использование электронной цифровой подписи. Содержание: Технологии аутентификации и шифрования; Реализация комплексной безопасной сетевой инфраструктуры для web-сервера. Хостинг во внешней организации. Сетевые элементы. IDS-системы и т.п. Действия для безопасности сетевой инфраструктуры. Восстановление при компрометации безопасности. Сканирование уязвимостей.	4	4		8	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос/доклад; тест
14	4.3. Технические средства защиты информации в ИС.	4	4		7,8	изучение теоретического материала; подготовка к практическим работам	практические задания; опрос/доклад; тест
	Итого за 8 семестр:	22	22		35,8		
	Всего часов:	**40**	**40**		**107,6**		