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

Утверждено:
на заседании кафедры
протокол№ 8 от « 24 » февраля 2021 г.
Зав. кафедрой _____ /Исмагилова А.С.

Согласовано:
Председатель УМК института
_____ / Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина
Защищенные информационные системы

Часть, формируемая участниками образовательных отношений (Б1.В.ДВ.01.01)

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) к.ф.-м.н., старший преподаватель кафедры управления информационной безопасностью	/ Юнусова Д.С.

Для приема: 2021 г.

Уфа 2021 г.

Составитель: Юнусова Дарья Сергеевна

Рабочая программа дисциплины *утверждена* на заседании кафедры протокол от «_24_» _февраля_____ 2021 г. № _8_

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

Заведующий кафедрой / 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

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**
Аналитическая	ПК-3. Способен анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации	ИПК-3.1 Знает принципы построения информационных систем	Знать принципы построения информационных систем
		ИПК-3.2 Умеет оценивать защищенность информационных систем	Уметь оценивать защищенность информационных систем
		ИПК-3.3 Владеет навыками анализа защищенности информационных систем	Владеть навыками анализа защищенности информационных систем
Организационно-управленческая	ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей	ИПК-1.1 Знает современные технологии построения безопасных информационных систем	Знать современные технологии построения безопасных информационных систем
		ИПК-1.2 Умеет анализировать и оценивать угрозы информационной безопасности	Уметь анализировать и оценивать угрозы информационной безопасности
		ИПК-1.3 Владеет методами формирования требований по защите информации	Владеть методами формирования требований по защите информации

2. Цель и место дисциплины в структуре образовательной программы

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

Дисциплина изучается на 5 курсе в 9 семестре.

Целью учебной дисциплины «Защищенные информационные системы» является получение базовых знаний в области теории и практики использования защищенных информационных систем.

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-3. Способен анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ИПК-3.1 Знает принципы построения информационных систем	Знать принципы построения информационных систем	Не знает принципы построения информационных систем	Имеет фрагментарные знания о принципах построения информационных систем	В целом знает принципы построения информационных систем	Знает принципы построения информационных систем
ИПК-3.2 Умеет оценивать защищенность информационных систем	Уметь оценивать защищенность информационных систем	Не умеет оценивать защищенность информационных систем	Умеет оценивать защищенность информационных систем, но допускает значительные ошибки	В целом умеет оценивать защищенность информационных систем, но допускает незначительные ошибки	Умеет оценивать защищенность информационных систем
ИПК-3.3 Владеет навыками анализа защищенности информационных систем	Владеть навыками анализа защищенности информационных систем	Не владеет навыками анализа защищенности информационных систем	Владеет навыками анализа защищенности информационных систем, но допускает значительные ошибки	Уверенно владеет навыками анализа защищенности информационных систем, но допускает незначительные ошибки	Владеет навыками анализа защищенности информационных систем

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 («Неудовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ИПК-1.1 Знает современные технологии построения безопасных информационных систем	Знать современные технологии построения безопасных информационных систем	Не знает современные технологии построения безопасных информационных систем	Имеет фрагментарные знания о современных технологиях построения безопасных информационных систем	В целом знает современные технологии построения безопасных информационных систем	Знает современные технологии построения безопасных информационных систем
ИПК-1.2 Умеет анализировать и оценивать угрозы информационной безопасности	Уметь анализировать и оценивать угрозы информационной безопасности	Не умеет анализировать и оценивать угрозы информационной безопасности	Умеет анализировать и оценивать угрозы информационной безопасности, но допускает значительные ошибки	В целом умеет анализировать и оценивать угрозы информационной безопасности, но допускает незначительные ошибки	Умеет анализировать и оценивать угрозы информационной безопасности
ИПК-1.3 Владеет методами формирования требований по защите информации	Владеть методами формирования требований по защите информации	Не владеет методами формирования требований по защите информации	Владеет методами формирования требований по защите информации, но допускает значительные ошибки	Уверенно владеет методами формирования требований по защите информации, но допускает незначительные ошибки	Владеет методами формирования требований по защите информации

Критериями оценивания 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).

Шкалы оценивания:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

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-3. Способен анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ИПК-3.1 Знает принципы построения информационных систем	Знать принципы построения информационных систем	тестирование, практическое задание
ИПК-3.2 Умеет оценивать защищенность информационных систем	Уметь оценивать защищенность информационных систем	тестирование, практическое задание
ИПК-3.3 Владеет навыками анализа защищенности информационных систем	Владеть навыками анализа защищенности информационных систем	тестирование, практическое задание

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
ИПК-1.1 Знает современные технологии построения безопасных информационных систем	Знать современные технологии построения безопасных информационных систем	тестирование, практическое задание
ИПК-1.2 Умеет анализировать и оценивать угрозы информационной безопасности	Уметь анализировать и оценивать угрозы информационной безопасности	тестирование, практическое задание
ИПК-1.3 Владеет методами формирования требований по защите информации	Владеть методами формирования требований по защите информации	тестирование, практическое задание

Рейтинг – план дисциплины
«Защищенные информационные системы»

Специальность: 10.05.05 Безопасность информационных технологий в правоохранительной сфере

курс 5, семестр 9

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Информационная система как объект защиты				
Текущий контроль				
Практическое задание	5	2	0	10
Рубежный контроль				
Тест	10	1	0	10
Всего			0	20
Модуль 2. Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем				
Текущий контроль				
Практическое задание	5	3	0	15
Рубежный контроль				
Тест	10	1	0	10
Всего			0	25
Модуль 3. Организационно-технические меры по реализации основных требований и построению системы информационной безопасности				
Текущий контроль				
Практическое задание	5	3	0	15
Рубежный контроль				
Тест	10	1	0	10
Всего			0	25
Поощрительные баллы				
1. Участие в студенческой олимпиаде	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции	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

Экзамен

Структура экзаменационного билета

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

Примерные вопросы к экзамену

1. Функционально-структурная организация информационных систем на архитектуре «клиент-сервер»
2. Определение основных приоритетов информационной безопасности в инфокоммуникационной системе
3. Функционально-структурная организация информационных систем на WEB-архитектуре
4. Модель нарушителя в инфокоммуникационной системе в закрытом контуре ЛВС
5. Структура построения политика информационной безопасности объекта защиты
6. Модель нарушителя в инфокоммуникационной системе в открытом контуре ЛВС
7. Описание объекта защиты. Определение основных приоритетов информационной безопасности
8. Значимые угрозы в инфокоммуникационной системе в закрытом контуре ЛВС
9. Значимые угрозы в инфокоммуникационной системе в открытом контуре ЛВС
10. Анализ рисков. Формирование перечня критичных ресурсов
11. Общие требования построения защищенной инфокоммуникационной системе
12. Требования к подсистеме резервирования и восстановления информации
13. Общие требования к подсистеме обеспечения безопасности сетевого взаимодействия
14. Требования к подсистеме контроля эталонного состояния информации и рабочей среды
15. Требования к подсистеме аутентификации и управления доступом
16. Требования к подсистеме управления безопасностью
17. Требования к подсистеме криптографической защиты информации
18. Требования к средствам построения защищенных сетей
19. Требования к подсистеме антивирусной защиты
20. Технические решения по защите от НСД межсетевого взаимодействия и передаваемой информации
21. Технические решения по защите от НСД компьютерных ресурсов на уровне серверов и рабочих станций ЛВС
22. Технические решения по реализации подсистемы аутентификации и идентификации

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.

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 Защищенные информационные системы

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Функционально-структурная организация информационных систем на архитектуре «клиент-сервер»
2. Общие требования построения защищенной инфокоммуникационной системе

Зав. Кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

Примерная тематика курсовых проектов (работ)

Курсовое проектирование не предусмотрено

Типовые 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.

Тест № 1
Модуль 1. Информационная система как объект защиты

Вопрос №1

Как называется модель, описывающая вероятный облик злоумышленника, т. е. его квалификацию, имеющиеся средства для реализации тех или иных атак, обычное время действия и т. п?

а) модель угрозы

б) модель нарушителя

в) модель безопасности

г) модель уязвимости

Вопрос №2

К какой угрозе можно отнести возможность ситуации, когда уволенный сотрудник беспрепятственно пользуется служебными полномочиями, в том числе корпоративным доступом в Интернет?

а) вредоносные программы

б) действия инсайдеров

в) хакерские атаки

г) спам

Вопрос №3

Выделите основные составляющие информационной безопасности.

а) целостность

б) доступность

в) полнота

г) конфиденциальность

д) актуальность

Тест № 2

Модуль 2. Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем

Вопрос №1

Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …

а) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды

б) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации

в) способна противостоять только информационным угрозам, как внешним так и внутренним

г) способна противостоять только внешним информационным угрозам

Вопрос №2

Сервисы безопасности:

а) идентификация и аутентификация

б) шифрование

в) инверсия паролей

г) контроль целостности

д) регулирование конфликтов

е) экранирование

ж) обеспечение безопасного восстановления

з) кэширование записей

Вопрос №3

Под угрозой удаленного администрирования в компьютерной сети понимается угроза

а) несанкционированного управления удаленным компьютером

б) внедрения агрессивного программного кода в рамках активных объектов Web-страниц

в) перехвата или подмены данных на путях транспортировки

г) вмешательства в личную жизнь; поставки неприемлемого содержания

Тест № 3

Модуль 3. Организационно-технические меры по реализации основных требований и построению системы информационной безопасности

Вопрос №1

К формам защиты информации не относится:

а) аналитическая

б) правовая

в) организационно-техническая

г) страховая

Вопрос №2

Наиболее эффективное средство для защиты от сетевых атак

а) использование сетевых экранов или «firewall»

б) использование антивирусных программ

в) посещение только «надёжных» Интернет-узлов

г) использование только сертифицированных программ-броузеров при доступе к сети Интернет

Вопрос №3

Защита информации обеспечивается применением антивирусных средств

а) да

б) нет

в) не всегда

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (20 вопросов в варианте)	Неправильный ответ / Правильный ответ	
Модуль 1		0,5
Модуль 2		0,5
Модуль 3		0,5

Комплект практических заданий

Для самостоятельного освоения и/или расширения знаний, умений, владений предусмотрены несколько практических занятий, к которым студенты должны подготовить доклады по темам практических занятий.

Темы практических занятий

1. Базовые принципы обеспечения безопасности локальной вычислительной сети
2. Информационная безопасность и защита информации
3. Методы обеспечения информационной безопасности
4. Комплексная защита информации на предприятии
5. Программно-аппаратные средства защиты информации от НСД
6. Использование межсетевых экранов для защиты локальных сетей
7. Сравнительный анализ операционных систем семейств Windows и Linux
8. Персональный сетевой экран
9. Интеллектуальная защита в режиме реального времени
10. Режим безопасного запуска программ
11. Предотвращение угроз, атак
12. Проверка веб-страниц, файлов и сообщений
13. Самозащита антивируса от попыток выключения со стороны вредоносного ПО
14. Защита конфиденциальных данных
15. Защита от кражи паролей, логинов и личных данных

Критерии оценивания

Практическое занятие оценивается в 5 баллов. Основными критериями при оценке практических занятий являются соответствие содержания доклада освещаемому вопросу, полнота раскрываемой в докладе темы, структура доклада и подача информации, а также правильные, аргументированные ответы на вопросы по докладу и степень участия в дискуссии.

5 баллов студент получает, если вопрос доклада освещен в полном объеме и изложен грамотным языком в правильной логической последовательности с точным использованием специализированной терминологии; если при этом показано уверенное владение материалом; студент правильно и аргументировано ответил на все вопросы по докладу и активно принимал участие в дискуссии.

4 балла студент получает, если вопрос доклада освещен в полном объеме, но имеются некоторые недостатки. К примеру, в работе допущены один-два недочета при освещении основного содержания ответа и/или нет определенной логической последовательности, неточно используется специализированная терминология или подача материала трудна для восприятия.

3 балла студент получает, если он не полно осветил вопрос, либо если доклад не структурирован, а также если студент не смог аргументировано ответить на вопросы по теме доклада.

2 балл студент получает, если он осветил вопрос неполно, не смог правильно ответить на вопросы по теме доклада.

1 балл студент получает, если содержание доклада соответствует теме освещаемого вопроса, но студент не показал общее понимание вопроса, не смог ответить на вопросы по теме доклада.

0 баллов студент получает при несоответствии содержания доклада освещаемому вопросу.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988

2. Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=429032

Дополнительная литература:

3. Ерохин, В. В. Безопасность информационных систем : учебное пособие : [16+] / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко. – 3-е изд., стер. – Москва : ФЛИНТА, 2016. – 184 с. : табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562458

4. Программно-аппаратные средства защиты информационных систем : учебное пособие : [16+] / Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 194 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499013

5. Артемов, А. В. Информационная безопасность: курс лекций / А. В. Артемов ; Межрегиональная академия безопасности и выживания. – Орел : Межрегиональная академия безопасности и выживания, 2014. – 257 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428605

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
2. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
3. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
4. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
5. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
6. www.newlibrary.ru – Новая электронная библиотека;
7. www. edu.ru – Федеральный портал российского образования;
8. www.elibrary.ru – Научная электронная библиотека;
9. www.nehudlit.ru – Электронная библиотека учебных материалов.
10. 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.
11. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
12. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

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

Наименование специальных помещений и помещений для самостоятельной работы	Вид занятий	Оснащенность специальных помещений и помещений для самостоятельной работы
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 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 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **3.** ***учебная аудитория для курсового проектирования (выполнения курсовых работ):*** аудитория № 613 (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	Лекции, практические занятия, текущий контроль, промежуточная аттестация	**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 AKG WMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром Promethean ActivBoard 387 RPO MOUNT EST -1 шт., Ком-ер встраиваемый в кафедру INTEL Core i3-4150/DDr3 4 Gb/HDD, Экран настенный Draper Luma AV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H – 1 шт. , Мультимедиа-проектор Panasonic PT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKG WMS45 – 1 шт. , Терминал видео конференц-связи LifeSize Icon 600 Camera 10x Phone 2nd Generation – 1 шт., Экран настенный Draper Luma AV(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 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 АРАРТ 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

(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 самостоятельной работы:*** аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).		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. **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. **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.

Приложение № 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Защищенные информационные системы** на 9 семестр
___очная_ф/о___

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	55,2
лекций	18
практических/ семинарских	36
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)	43,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к зачету (Контроль)	45

Форма контроля
Экзамен 9 семестр

Семестр 9

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛР	СРС		
1	2	3	4	5	6	8	9
Модуль 1. Информационная система как объект защиты							
1	Эволюция архитектур информационных систем. Политика информационной безопасности объекта защиты. Описание объекта защиты.	2	4		3,8	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
2	Определение основных приоритетов информационной безопасности. Анализ рисков.	2	4		5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
3	Формирование перечня критичных ресурсов. Модели нарушителя и угроз.	2	4		5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
Модуль 2. Требования информационной безопасности в закрытых и открытых контурах локальной вычислительной сети инфокоммуникационных систем							
4	Общие требования построения защищенной информационной системы. Требования к подсистеме обеспечения безопасности сетевого взаимодействия.	2	4		5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование

5	Требования к подсистеме аутентификации и управления доступом. Требования к подсистемам криптографической защиты информации и антивирусной защиты.	2	4		5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
6	Требования к подсистемам резервирования/ восстановления информации, контроля эталонного состояния информации и рабочей среды. Требования к средствам построения защищенных сетей и управления безопасностью.	2	4		5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
Модуль 3. Организационно-технические меры по реализации основных требований и построению системы информационной безопасности							
7	Многоуровневая модель защиты в информационной системе на архитектуре «клиент-сервер»: методы защиты информации на физическом, канальном, сетевом, транспортном, сеансовом и прикладном уровнях модели. Протокол формирования защищенного туннеля на канальном уровне.	2	4		5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
8	Технические решения по защите межсетевого взаимодействия и передачи информации. Средства криптографической защиты информации.	2	4		5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
9	Технические решения по защите от вредоносного кода. Технические решения по защите от НСД компьютерных ресурсов на уровне серверов и рабочих станций ЛВС и реализации подсистемы аутентификации и идентификации	2	4		5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Практическая работа, тестирование
Всего часов:		18	36		43,8		