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
Информационная безопасность автоматизированных систем

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

программа магистратуры

Направление подготовки
10.04.01 Информационная безопасность

Направленность подготовки (программа магистратуры)
Информационная безопасность цифровых технологий

Квалификация
магистр

Разработчики: К.филос.н., доц. каф. Управления информационной безопасностью; ст. преподаватель каф. УИБ	_____ / Миронова Н.Г. _____ / Салов И.В.

Для приема: 2021 г.

Уфа 2021 г.

Составители: к.филос.н. Миронова Наталия Геннадьевна, Салов Игорь Владимирович

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**
	ПК-3 Способен анализировать и обобщать результаты научных исследований и разработок в области автоматизации информационно-аналитической деятельности	ПК 3.1. Знает методы анализа результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	Знать методы анализа результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.
		ПК 3.2. Умеет применять методы анализа и обобщения результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	Уметь применять методы анализа и обобщения результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.
		ПК 3.3. Владеет технологией анализа и обобщения результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	Владеть технологией анализа и обобщения результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность автоматизированных систем» относится к части, формируемой участниками образовательных отношений, дисциплинам по выбору.

Дисциплина изучается на 1 курсе магистратуры в 1 семестре.

Целью учебной дисциплины «Информационная безопасность автоматизированных систем» является формирование навыков анализа и обобщения результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.

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 и обобщать результаты научных исследований и разработок в области автоматизации информационно-аналитической деятельности.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК 3.1. Знает методы анализа результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	Знать методы анализа результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	Не знает или показывает очень слабые знания.	Слабо знает указанные требования и технологии, имеет фрагментарные знания.	Демонстрирует хорошее знание указанных требований и технологий, но не всегда способен увязать их с практикой защиты информации в АС.	Демонстрирует целостные, системные знания в указанной сфере.
ПК 3.2. Умеет применять методы анализа и обобщения результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	Уметь применять методы анализа и обобщения результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	Не умеет.	Слабо демонстрирует указанные умения и знания, без связи навыками решения задач защиты информации в АС.	Демонстрирует хорошее теоретическое знание компетенции, но недостаточное владение практической стороной при решении задач защиты информации в АС	Демонстрирует уверенное, свободное владение указанными навыками при решении задач организации защиты информации в АС
ПК 3.3. Владеет технологией анализа и обобщения	Владеть технологией анализа и обобщения	Не владеет.	Слабо демонстрирует указанные	Демонстрирует хорошее владение	Демонстрирует уверенное, свободное

результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.		навыки.	компетенцией, но допускает мелкие ошибки.	владение указанными навыками при решении задач защиты информации в 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-3. Способен анализировать и обобщать результаты научных исследований и разработок в области автоматизации информационно-аналитической деятельности.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ПК 3.1. Знает методы анализа результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	Знать методы анализа результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	тестирование, практическое задание
ПК 3.2. Умеет применять методы анализа и обобщения результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	Уметь применять методы анализа и обобщения результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	тестирование, практическое задание
ПК 3.3. Владеет технологией анализа и обобщения результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	Владеть технологией анализа и обобщения результатов научных исследований и разработок в области автоматизации информационно-аналитической деятельности.	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.

Шкалы оценивания для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

Рейтинг – план дисциплины
«Информационная безопасность автоматизированных систем»

Специальность: 10.04.01 Информационная безопасность

курс 1, семестр 1

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				
Лабораторная работа	3	4	0	12
Практическая работа	3	4	0	12
Рубежный контроль				
Тест	16	1	0	16
Всего			0	40
Модуль 2. Методы, модели и механизмы обеспечения целостности и правомерной доступности данных.				
Текущий контроль				
Лабораторная работа	3	4	0	12
Практическая работа	3	4	0	12
Рубежный контроль				
Тест	6	1	0	6
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

Экзамен

Структура экзаменационного билета

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

Типовые экзаменационные вопросы:

1. Концепция информационной безопасности организации.
2. Нормативные документы и ГОСТы по обеспечению информационной безопасности АС.

3. План защиты информации.
4. План обеспечения непрерывной работы и восстановления подсистем автоматизированной системы.
5. Назначение и возможности средств защиты информации от несанкционированного доступа.
6. Основные механизмы защиты автоматизированных систем.
7. Защита периметра компьютерных сетей и управление механизмами защиты.
8. Страхование информационных рисков.
9. Аппаратно-программные средства защиты информации от несанкционированного доступа.
10. Рекомендации по выбору средств защиты информации от несанкционированного доступа.
11. Обзор существующих на рынке средств защиты информации от несанкционированного доступа.
12. Средства аппаратной поддержки.
13. Способы аутентификации.
14. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа
15. Стратегия безопасности Microsoft.
16. Защита от вмешательства в процесс нормального функционирования автоматизированной системы.
17. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы.
18. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа.
19. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.
20. Угрозы информационной безопасности автоматизированных системы.
21. Обеспечение безопасности компьютерных сетей.
22. Проблемы обеспечения безопасности в компьютерных сетях.
23. Типовая корпоративная сеть.
24. Уровни информационной инфраструктуры корпоративной сети.
25. Уязвимости и их классификация.
26. Классификация атак.
27. Средства защиты сетей. Защита периметра корпоративной сети.
28. Угрозы, связанные с периметром корпоративной сети. Составляющие защиты периметра.
29. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности.
30. Управление уязвимостями. Архитектура систем управления уязвимостями.
31. Особенности сетевых агентов сканирования.
32. Средства анализа защищенности системного уровня.
33. Мониторинг событий безопасности
34. Введение в управление журналами событий. Категории журналов событий. Инфраструктура управления журналами событий.
35. Введение в технологию обнаружения атак. Классификация систем обнаружения атак.
36. Распределение функций по обеспечению безопасности автоматизированных систем.
37. Организационно-распорядительные документы по обеспечению безопасности автоматизированных систем.
38. Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях
39. Проблема человеческого фактора. Общие правила обеспечения безопасности.
40. Обязанности ответственного за обеспечение безопасности информации в подразделении. Ответственность за нарушения требований обеспечения безопасности.

41. Порядок работы с носителями ключевой информации.
42. Регламентация работ по обеспечению безопасности автоматизированных систем. Регламентация порядка допуска к работе и изменения полномочий пользователей автоматизированной системы.
43. Регламентация порядка изменения конфигурации аппаратно-программных средств автоматизированной системы. Регламентация правил парольной и антивирусной защиты.
44. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач.
45. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов.
46. Категорирование защищаемых ресурсов.
47. Проведение информационных обследований и документирование защищаемых ресурсов.
48. Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем автоматизированной системы.

Пример экзаменационного билета:

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

Специальность 10.04.01 Информационная безопасность

Дисциплина Информационная безопасность автоматизированных систем

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Регламентация порядка допуска к работе и изменения полномочий пользователей автоматизированной системы.
2. Инфраструктура управления журналами событий.

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 четырех-балльную:

- 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

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.
В вопросах закрытого типа следует выбрать один верный ответ из предложенных вариантов.

Модуль 1. Общая характеристика информационной защиты автоматизированных систем

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

и т.д. подробнее см. в ФОС дисциплины.

Модуль 2. Методы, модели и механизмы обеспечения целостности и правомерной доступности данных

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) Из перечисленного ACL-список содержит:
а) срок действия маркера доступа;
б) домены, которым разрешен доступ к объекту;

4) Из перечисленного в ОС UNIX существуют администраторы:
а) системных утилит;
б) службы контроля;
в) службы аутентификации;
г) тиражирования;
д) печати;
е) аудита

и т.д. подробнее см. в ФОС дисциплины.

Критерии оценки тестовых заданий (в каждом из 2-х тестов - 25 вопросов):

- Тест по результату освоения Модуля 1 (до 0,64 балла за правильный ответ на тестовый вопрос, 0 – за неправильный ответ).
- Тест по результату освоения Модуля 2 (до 0,24 балла за правильный ответ на тестовый вопрос, 0 – за неправильный ответ).

Типовые практические и лабораторные задания

Цель проведения практических работ – практическое освоение материала дисциплины.

Темы практических работ

1) Анализ угроз информационной безопасности (2 часа).
2) Классификация ПАСОИБ (2 часа).
3) Методы криптографической защиты (2 часа).
4) Журналы регистрации событий на примере ОС Windows (2 часа).
5) Программно-аппаратные средства защиты от несанкционированного доступа к информации, хранимой в ПЭВМ (2 часа).
6) Система контроля и управления доступом (СКУД) на примере гуманитарного корпуса БашГУ (2 часа).

7) Системы сигнализации на примере гуманитарного корпуса БашГУ (2 часа).
8) Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи (4 часа).

Типовые задания практических работ

Типовая практическая работа №1. Анализ угроз информационной безопасности (2 часа)

Цель: На практике ознакомиться с анализом угроз информационной безопасности организации.

Задание: Провести на практике анализ угроз информационной безопасности организации.

Порядок выполнения:

1) Изучите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Методы и средства обеспечения безопасности. Часть 3 «Методы менеджмента безопасности информационных технологий».
2) Ознакомьтесь с Приложениями C, D и E ГОСТа.
3) Выберите один из различных информационных актива организации.
4) Из Приложения D ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
5) Пользуясь Приложением C ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.
6) Пользуясь одним из методов предложенных в Приложении E ГОСТа произведите оценку рисков информационной безопасности.
7) Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

Критерии оценки практической работы:

Структура работы	Критерии оценки	Распределение баллов
Одно практическое задание Модуль 1 Модуль 2	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

Типовые задания лабораторных работ

Цель проведения лабораторных работы – практическое освоение материала дисциплины.

Темы лабораторных работ

1) Система защиты СЗИ DallasLock (2 часа).
2) Механизмы управления доступом и защиты объектов в системе DallasLock (2 часа).
3) Аудит безопасности средствами СЗИ DallasLock (2 часа)..
4) Построение СЗИ от НСД по нормативным требованиям ФСТЭК (2 часа).
5) Система защиты информации «SecretNet» (2 часа).
6) Обеспечение разграничения доступа к защищаемой информации средствами «SecretNet» (2 часа).
7) Построение системы защиты на базе СЗИ «SecretNet» (2 часа).

8) Управление ресурсами в «Страж NT»: управление доступом, штамп, аудит, целостность, режим запуска (4 часа).

Типовая лабораторная работа № 1. Система защиты СЗИ DallasLock (2 часа)

Цель: Изучить основные функции СЗИ DallasLock.
Содержание: Выполнение заданий:

Порядок выполнения:

1. По каналу связи передается пять сообщений, вероятность получения первого Изучить «Руководство по эксплуатации СЗИ Dallas Lock 8.0» RU.48957919.501410-01 92 и RU.48957919.501410-02 92.
2. Изучить «Описание применения СЗИ Dallas Lock 8.0» RU.48957919.501410-01 31 и RU.48957919.501410-02 31.
3. Убедиться, что лабораторный компьютер соответствует минимальным требованиям по применению СЗИ Dallas Lock 8.0.
4. Установить СЗИ Dallas Lock 8.0К.
5. Настроить СЗИ Dallas Lock 8.0К.
6. Деинсталлировать СЗИ Dallas Lock 8.0К.
7. Ответить на контрольные вопросы:
   a) Что такое дескриптор объекта в DL 8.0?
   b) Для чего он используется?
   c) Какие типы дескрипторов бывают.
   d) На какие разряды можно разделить всех пользователей, зарегистрированных в системе защиты DL 8.0, применительно к правам доступа?
   e) Какие операции можно производить с объектом в системе защиты DL 8.0 в зависимости от типа объекта?
8. Защита лабораторной работы. Проводится в форме устного опроса после выполнения работы.

И т.д. см. подробнее ФОС дисциплины.

Критерии оценки лабораторной работы:

- 0 баллов – если работа выполнена с ошибками и не получены ответы на все контрольные вопросы
- 2 балла - если работа выполнена, но не получены ответы на все контрольные вопросы
- 4 балла - работа выполнена и получены ответы на все контрольные вопросы.

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
3. Прошин, И. А. Проектирование автоматизированных систем : учебное пособие / И. А. Прошин, Л. Ю. Акулова, В. Н.
4. Прошкин. — Пенза : ПензГТУ, 2012. — 274 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/62649.
5. Прошин, Д. И. Автоматизированная обработка информации в системах управления технологическими процессами: учебное пособие / Д. И. Прошин. — Пенза : ПензГТУ, 2012. — 113 с. — Текст : электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/62505.
6. Давидюк, Н. В. Разработка автоматизированных систем обработки информации в защищенном исполнении: учебное пособие / Н. В. Давидюк. — Санкт-Петербург : Интермедия, 2020. — 48 с. — ISBN 978-5-4383-0194-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/161365.
7. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
8. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».
9. ГОСТ Р 56093-2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Средства
   обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования»
10. ГОСТ Р 56103-2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения».
11. ГОСТ Р 56115-2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования».
12. ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей».
13. ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем».
14. ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения».
15. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
16. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

17. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важныхобъектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
18. Приказ ФСТЭК России от 29 апреля 2021 г. N 77 «Об утверждении порядка организации и проведения работ по
аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

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 East View) - 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 East View) (вход без регистрации). - Ссылка http://www.ebiblioteka.ru/browse/udb/12.
3. Annual Reviews – обзор журналов по общественно-научной тематике и др. – доступ из сети вуза. – Ссылка: http://www.annualreviews.org/
4. Computers & Applied Sciences Complete (EBSCO) - доступ в сети вуза, язык английский. - 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. Taylor and Francis – База полнотекстовых научных журналов, книг. Язык английский. – доступ из сети вуза. – Ссылка: http://www.tandf
7. Web of Science - наукометрическая, библиографическая и реферативная база данных издательской корпорации Thomson Reuters. 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

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. Лицензии бессрочные.
4. 1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях. Договор № 1199 от 09.01.2019 г.

5. Система DirectumRX (ежегодно пролонгируемый договор с компанией Directum (Ижевск) о предоставлении бесплатного учебного доступа к облачной платформе).
6. Project Expert 7 Tutorial. Договор № 263 от 07.12.2012 г.

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 № 515.	Лекции,	**Аудитория № 515.** Оборудование: учебная мебель, доска, терминал видео конференц-связи LifeSizeIcon 600-камера, интерактивная система со встроенным короткофокусным проектором PrometheanActivBoard 387 RPOMOUNTEST, профессиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMARTPodiumSP518 с ПО SMARTNotebook, матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H, интерактивная напольная кафедра докладчика, ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/ThermaltakeVL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Перечень лицензионного программного обеспечения:** 1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.
2**. Учебная аудитория для проведения занятий семинарского типа:** Аудитория № 417. Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации. Аудитория № 508. Специализированная аудитория с лабораторным оборудованием. Аудитория № 509. Лаборатория моделирования процессов защиты	лабораторные и практические занятия	**Аудитория № 417. Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.** Оборудование: учебная мебель, доска, комплект учебного оборудования «Блочное кодирование», комплект учебного оборудования «Основы криптографии», учебно-лабораторный стенд «Аттестация объекта информатизации по требованиям защиты от утечек по каналу побочных ЭМИ» **Аудитория № 508. Специализированная аудитория с лабораторным оборудованием.** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, учебно-демонстрационная панель «Монтаж средств технической защиты информации» **Аудитория № 509. Лаборатория моделирования процессов защиты информации.** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, учебно-лабораторный стенд «Сетевая безопасность».

информации.		
3. Учебная аудитория для проведения групповых и индивидуальных консультаций: Аудитория № 608 4. Учебная аудитория для текущего контроля и промежуточной аттестации: Аудитория № 609 Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование.	Консультации, текущий контроль, промежуточная аттестация	**Аудитория № 608** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, телевизор TCL-L55P6US. **Аудитория № 609** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование. Перечень лицензионного программного обеспечения: 1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License. 4. 1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях. Договор № 1199 от 09.01.2019 г. 5. Система DirectumRX (ежегодно пролонгируемый договор с компанией Directum (Ижевск) о предоставлении бесплатного учебного доступа к облачной платформе).

Приложение 1.

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Информационная безопасность автоматизированных систем** на 1 семестр

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	55,2
лекций	18
практических/ семинарских	18
лабораторных	18
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)	16,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к экзамену (Контроль)	36

Форма контроля
Экзамен 1 семестр

Семестр 1

№	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.	2	2	2	1	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;
	Тема: Правовые основы обеспечения безопасности автоматизировании систем. Защищаемая информация.	2	2	2	1,8	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;
	Тема: Организационная структура системы обеспечения безопасности автоматизированных систем.	2	2	2	2	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;
	Тема: Регламентация работ по обеспечению безопасности автоматизированных систем.	2	2	2	2	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;
2	**Модуль 2. Методы, модели и механизмы обеспечения целостности и правомерной доступности данных.**						
	Тема: Назначение и возможности средств защиты	2	–	–	2	изучение	

	информации от несанкционированного доступа.					теоретического материала; подготовка к практическим работам	
	Тема: Применение штатных и дополнительных средств защиты информации от несанкционированного доступа.	2	2	2	2	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;
	Тема: Обеспечение безопасности компьютерных сетей.	2	2	2	2	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;
	Тема: Обнаружение и устранение уязвимостей.	2	2	2	2	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;
	Тема: Мероприятия по обеспечению информационной безопасности в компьютерных сетях.	2	4	4	2	изучение теоретического материала; подготовка к практическим работам	Практические и лабораторные задания, тест;
Всего часов		18	18	18	16,8		