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 факультета /института

_____/Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина
Моделирование процессов и систем защиты информации (Б1.В.04)
базовая часть

программа магистратуры

Направление подготовки
10.04.01 Информационная безопасность

Направленность (профиль) подготовки
Информационная безопасность цифровых технологий

Квалификация
магистр

Разработчик (составитель) доцент кафедры, к. филос. н. (должность, ученая степень, ученое звание)	_____ / Миронова Н.Г.

Для приема: 2021

Уфа 2021 г.

Составитель: Миронова 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 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**
Командная работа и лидерство	УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели;	УК 3.1. Знает: способы подбора эффективной команды; основные условия эффективной командной работы; стратегии и принципы командной работы; основы психологии личности, среды, группы, коллектива	Знать способы подбора эффективной команды; основные условия эффективной командной работы; стратегии и принципы командной работы; основы психологии личности, среды, группы, коллектива
		УК 3.2. Умеет: вырабатывать командную стратегию; применять принципы и методы организации командной деятельности	Уметь вырабатывать командную стратегию; применять принципы и методы организации командной деятельности
		УК 3.3. Владеет: навыками социального взаимодействия и реализации своей роли в команде; создания команды для выполнения практических задач; участия в разработке стратегии командной работы	Владеть навыками социального взаимодействия и реализации своей роли в команде; создания команды для выполнения практических задач; участия в разработке стратегии командной работы
	ПК-2. Способен разрабатывать проектные решения по защите информации в автоматизированных системах	ПК-2.1. Знает основные методы разработки проектных решений по защите информации в автоматизированных системах	Знать основные методы разработки проектных решений по защите информации в автоматизированных системах
		ПК-2.4. Умеет применять основные методы и технологии разработки проектных решений по защите информации в автоматизированных системах	Уметь применять основные методы и технологии разработки проектных решений по защите информации в автоматизированных системах
		ПК-2.7. Способен участвовать в разработке проектных решений по защите информации в автоматизированных системах	Владеть способностью принимать продуктивное участие в разработке проектных решений по защите информации в автоматизированных системах

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Моделирование процессов и систем защиты информации» относится к части, формируемой участниками образовательных отношений.

Дисциплина изучается на 2 курсе в 4 семестре.

Цели изучения дисциплины «Моделирование процессов и систем защиты информации» - знакомство с принципами и методами моделирования процессов для разработки проектных решений по защите информации в автоматизированных системах, получение практических навыков моделирования процессов и систем защиты информации для автоматизированных 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.

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели;

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
УК 3.1. Знает: способы подбора эффективной команды; основные условия эффективной командной работы; стратегии и принципы командной работы; основы психологии личности, среды, группы, коллектива	Знать способы подбора эффективной команды; основные условия эффективной командной работы; стратегии и принципы командной работы; основы психологии личности, среды, группы, коллектива	Не знает	Слабо знает указанные понятия, способы и принципы.	Демонстрирует хорошее знание указанных понятий, способов и принципов, но не всегда способен увязать их с практикой проектирования системы защиты информации.	Демонстрирует целостные, системные знания в указанной сфере.
УК 3.2. Умеет: вырабатывать командную стратегию; применять принципы и	Уметь вырабатывать командную стратегию; применять	Не умеет	Слабо демонстрирует указанные умения и знания, без	Демонстрирует хорошее теоретическое знание компетенции,	Демонстрирует уверенное, свободное владение указанными

методы организации командной деятельности	принципы и методы организации командной деятельности		связи навыками решения задач организации службы защиты информации.	но недостаточное владение практической стороной при решении задач проектирования системы защиты информации	навыками при решении задач проектирования системы защиты информации
УК 3.3. Владеет: навыками социального взаимодействия и реализации своей роли в команде; создания команды для выполнения практических задач; участия в разработке стратегии командной работы	Владеть навыками социального взаимодействия и реализации своей роли в команде; создания команды для выполнения практических задач; участия в разработке стратегии командной работы	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 проектирования системы защиты информации.

ПК-2. Способен разрабатывать проектные решения по защите информации в автоматизированных системах.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК-2.1. Знает основные методы разработки проектных решений по защите информации в автоматизированных системах	Знать основные методы разработки проектных решений по защите информации в автоматизированных системах	Не знает	Слабо знает указанные понятия, способы и принципы.	Демонстрирует хорошее знание указанных понятий, способов и принципов, но не всегда способен увязать их с практикой проектирования системы защиты информации.	Демонстрирует целостные, системные знания в указанной сфере.
ПК-2.4. Умеет применять основные методы и технологии разработки проектных решений по защите информации в автоматизирова	Уметь применять основные методы и технологии разработки проектных решений по защите информации в автоматизиров	Не умеет	Слабо демонстрирует указанные умения и знания, без связи навыками решения задач организации службы	Демонстрирует хорошее теоретическое знание компетенции, но недостаточное владение практической стороной при	Демонстрирует уверенное, свободное владение указанными навыками при решении задач проектирования системы защиты

нных системах	анных системах		защиты информации.	решении задач проектирования системы защиты информации	информации
ПК-2.7. Способен участвовать в разработке проектных решений по защите информации в автоматизированных системах	Владеть способностью принимать продуктивное участие в разработке проектных решений по защите информации в автоматизированных системах	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 проектирования системы защиты информации.

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

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели;

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
УК 3.1. Знает: способы подбора эффективной команды; основные условия эффективной командной работы; стратегии и принципы командной работы; основы психологии личности, среды, группы, коллектива	Знать способы подбора эффективной команды; основные условия эффективной командной работы; стратегии и принципы командной работы; основы психологии личности, среды, группы, коллектива	практические задания; опрос/доклад; отчет по контрольным работам; компьютерный тест;
УК 3.2. Умеет: вырабатывать командную стратегию; применять принципы и методы организации командной деятельности	Уметь вырабатывать командную стратегию; применять принципы и методы организации командной деятельности	практические задания; опрос/доклад; отчет по контрольным работам; компьютерный тест;
УК 3.3. Владеет: навыками социального взаимодействия и реализации своей роли в команде; создания команды для выполнения практических задач; участия в разработке стратегии командной работы	Владеть навыками социального взаимодействия и реализации своей роли в команде; создания команды для выполнения практических задач; участия в разработке стратегии командной работы	практические задания; опрос/доклад; отчет по контрольным работам;

ПК-2. Способен разрабатывать проектные решения по защите информации в автоматизированных системах.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ПК-2.1. Знает основные методы разработки проектных решений по защите информации в автоматизированных системах	Знать основные методы разработки проектных решений по защите информации в автоматизированных системах	практические задания; опрос/доклад; отчет по контрольным работам; компьютерный тест;
ПК-2.4. Умеет применять основные методы и технологии разработки проектных решений по защите информации в автоматизированных системах	Уметь применять основные методы и технологии разработки проектных решений по защите информации в автоматизированных системах	практические задания; опрос/доклад; отчет по контрольным работам; компьютерный тест;
ПК-2.7. Способен участвовать в разработке проектных решений по защите информации в автоматизированных системах	Владеть способностью принимать продуктивное участие в разработке проектных решений по защите информации в автоматизированных системах	практические задания; опрос/доклад; отчет по контрольным работам;

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.

Шкалы оценивания:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

Рейтинг – план дисциплины
«Моделирование процессов и систем защиты информации»

Направление подготовки 10.04.01 Информационная безопасность

курс 2, семестр 4

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль				
1. Аудиторная работа	5	2	0	10
Рубежный контроль				
1. Письменная контрольная работа	10	1	0	10
Модуль 2				
Текущий контроль				
1. Аудиторная работа	5	6	0	30
3. ..				
Рубежный контроль				
1. Тестовый контроль	10	1	0	10
2. Письменная контрольная работа	10	1	0	10
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. Классификация моделей.
2. Системный подход к защите информации.
3. Системные принципы создания комплексной защиты информации.
4. Выбор уровня описания системы в модели.
5. Этапы моделирования.
6. Виды показателей эффективности.
7. Методы определения важности требований, предъявляемых к системе защиты информации.
8. Выбор уровня описания системы в модели.
9. Алгоритм создания системы комплексной защиты.
10. Методология разработки моделей.
11. Модели процессов в информационном обмене в системах защиты информации.
12. Функции моделирования информационного обмена.
13. Способ перехода от математической модели процесса к цифровой модели.
14. Определение динамических диапазонов модулируемых процессов.
15. Методы оценки адекватности, устойчивости, чувствительности модели.
16. Модель представления информации с учетом надежности программно-аппаратных средств.
17. Разработка модели управления рисками информационной безопасности.
18. Модель процессов контроля информации.
19. Модель процессов воздействия компьютерных вирусов.
20. Разработка модели действий инсайдера.
21. Модель процессов сохранения конфиденциальности информации.
22. Модель синтеза рационального проекта системы защиты информации.
23. Модель адаптивной системы информационной безопасности.
24. Модель злоумышленника (какими нормативными документами регламентируется создание, что входит в модель, порядок ее разработки).
25. Проблемы импортозамещения средств разработки систем защиты информации и систем защиты информации

Образец экзаменационного билета:

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

Направление подготовки 10.04.01 «Информационная безопасность»

Дисциплина: Моделирование процессов и систем защиты информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 10

1. Функции моделирования информационного обмена.
2. Методология разработки моделей.

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 практических занятий

Раздел 1. Подходы и методологии моделирования процессов и систем

Типовое практическое занятие № 1. Методологии моделирования процессов и систем (2 часа)

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

1. Классификация методов моделирования.
2. Принципы системного подхода в моделировании.
3. Подходы и методологии моделирования процессов и систем.
4. Выбор уровня описания системы в модели. Этапы моделирования.
5. Выбор уровня описания системы в модели. Методология разработки моделей. Графические нотации (языки) для описания процессов и системы
6. Программные средства для проектирования процессов и систем защиты информации.

Практическая часть

Выполнение практического задания по теме практики (проектирование типового рабочего процесса по ЗИ с помощью средств или сервисов графического проектирования).

Типовое практическое занятие № 2. Графические нотации и средства моделирования процессов и проектирования систем защиты информации (СЗИ) (2 часа)

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

1. Системные принципы создания комплексной защиты информации.
2. Принципы проектирования СЗИ.
3. Алгоритм создания системы комплексной защиты.
4. Виды показателей эффективности СЗИ.
5. Этапы проектирования СЗИ.
6. Графические нотации и средства моделирования процессов и проектирования систем защиты информации (СЗИ).

Практическая часть

1. Распределение заданий для выполнения самостоятельной контрольной работы №1
2. Выполнение практического задания по теме практики (проектирование элемента СЗИ с помощью средств или сервисов графического проектирования).

Раздел 2. Практика моделирования процессов и систем защиты информации.

Типовое практическое занятие № 3. Моделирование угроз: модель процессов воздействия компьютерных вирусов; модели нарушителя/злоумышленника (2 часа)

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

1. Моделирование угроз: модель процессов воздействия компьютерных вирусов
2. Моделирование угроз: модели нарушителя/злоумышленника.

Практическая часть
Выполнение практического задания по теме практики (моделирование процесса реализации угрозы (по заданию, по вариантам)).

Типовое практическое занятие № 4. Модель представления информации с учетом надежности программно-аппаратных средств (2 часа)

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

1. Системный подход к управлению защитой информации. Системные принципы создания комплексной защиты информации.
2. Модель формирования множества функций защиты информации.
3. Показатели надежности программно-аппаратных средств.

Практическая часть
Выполнение практического задания по теме практики (по заданию, по вариантам)

1. Моделирование представления информации
2. Создание модели нарушителя (или модели действий инсайдера).

Типовое практическое занятие № 5. Моделирование рисков информационной безопасности. Модель процессов сохранения конфиденциальности информации. Модель процессов контроля информации (2 часа)

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

1. Риски информационной безопасности и управление ими.
2. Проблема оценки рисков (методы оценки вероятностей реализации угроз, методологии расчетов).
3. Моделирование случайных факторов.
4. Модель управления рисками информационной безопасности
5. Показатели надежности программно-аппаратных средств.
6. Модель процессов сохранения конфиденциальности информации.
7. Модель процессов контроля информации
8. Модель процессов сохранения конфиденциальности информации.
9. Модель процессов контроля информации

Практическая часть
Выполнение практического задания по теме практики (моделирование) по заданию.
Разработка модели управления рисками информационной безопасности.

Типовое практическое занятие № 6. Методы проектирования (в т.ч. СЗИ). Методы оценки адекватности, устойчивости, чувствительности модели (2 часа)

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

Теоретическая часть:

1. Виды показателей эффективности.
3. Метод обобщенного показателя.
4. Метод «затраты-эффект».
5. Метод целевого программирования.
1. Методы теории игр в информационной безопасности.
2. Метод интерпретации.
3. Виды представления времени в модели.
4. Моделирование по событиям. Моделирование параллельных процессов.
5. Модели выбора рационального варианта средства защиты информации на основе экспертной информации.
6. Вероятностная модель системы контроля доступа к информации.
7. Модель на основе нейронных сетей в задачах защиты информации.

Типовое практическое занятие № 7. Модель системы защиты информации; адаптивность системы информационной безопасности (2 часа)

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

1. Методы определения важности требований к процессам и системам защиты информации.
2. Модель адаптивной системы информационной безопасности.

Практическая часть
Разработка модели защиты информации.

Типовое практическое занятие 8. Об имитационном моделировании как методе проектирования СЗИ. Тестирование (2 часа)

Содержание:

1. Имитационное моделирование при разработке системы защиты информации.
2. Стратегическое планирование имитационного экспериментов.
3. Тактическое планирование имитационного экспериментов.
4. Оценка качества имитационной модели. Методы оценки адекватности.
5. Методы оценки адекватности, устойчивости, чувствительности модели.
6. Методы оценки чувствительности модели.
7. Калибровка модели.
8. Оценка влияния и взаимосвязи факторов.

Итоговое тестирование

Критерии оценки результатов выполнения заданий практических занятий (в баллах*):*

- 5 баллов выставляется студенту, если работа практического занятия выполнена без ошибок и без замечаний (если занятие проводится в форме семинара – за доклад, раскрывающий тему и содержащий актуальные сведения, сопровождаемый презентацией);
- 3-4 балла выставляется студенту, если работа выполнена с ошибками и/или поставленная в задаче цель достигнута частично (60-90%);
- 1-2 балла выставляется студенту, если работа выполнена с ошибками и/или поставленная в задаче цель достигнута частично (30-60%).

Типовые задания для контрольной работы

Описание контрольной работы:

В течение курса проводятся 2 письменные контрольные работы по результатам разделов№ 1 и №2. Контрольные работы проводятся в письменной форме (электронный отчет с ответом на вопрос (тему), доставшийся студенту случайным образом из нижеприведенного списка). Отчеты по обеим контрольным работам должны быть предоставлен в отведенный срок (сообщается студентам при раздаче заданий) и размещен в СДО или прислан по электронной почте и т.п. образом. Критерии оценки приводятся ниже. Оформление – типичное для контрольных работ (см. методуказания по оформлению учебных контрольных работ на сайте БашГУ в разделе для студентов).

Пример варианта контрольной работы №1

1. Основы теории моделирования. Основные термины и определения . Классификация методов моделирования.
2. Принципы системного подхода в моделировании.
3. Виды показателей эффективности. Метод обобщенного показателя. Метод «затраты-эффект». Метод целевого программирования.
4. Системный подход к управлению защитой информации. Системные принципы создания комплексной защиты информации.
5. Выбор уровня описания системы в модели. Этапы моделирования.
6. Выбор уровня описания системы в модели. Методология разработки моделей. Алгоритм создания системы комплексной защиты.
7. Модель формирования множества функций защиты информации.

Пример варианта контрольной работы № 2

1. Моделирование случайных факторов.
2. Метод интерпретации.
3. Модель нарушителя.
4. Виды представления времени в модели.
5. Моделирование по событиям. Моделирование параллельных процессов.
6. Модели выбора рационального варианта средства защиты информации на основе экспертной информации.

Описание методики оценивания:

Каждая из 2-х контрольных работ оценивается максимально в 10 баллов.

Критерии оценки (в баллах) каждой из двух контрольных работ:

- до 2 баллов выставляется студенту, если отчет предоставлен после истечения отведенного срока и выполнен с грубыми ошибками(содержание вопроса не раскрыто или раскрыто неверно, источники для ответа не указаны вообще);
- от 3 до 6 баллов выставляется студенту, если отчет не сдан вовремя или тема не раскрыта в должной мере, материалы устарели, источники указаны неполно;
- от 6 до 8 баллов выставляется студенту, если отчет сдан вовремя, тема раскрыта, источники указаны, но не являются достоверными и актуальными, а также оформение отчета свидетельствует о недостаточном освоении материала, термины используются не всегда корректно ;
- от 8 до 10 баллов выставляется студенту, если отчет по контрольной работе сдан в срок, ответ на вопрос дан в полной мере. материалы актуальны и содержат сылки на источники, однако ответ недостаточно лаконичен (имеется избыточная информация) или имеются мелкие ошибки в оформлении.

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 или в личном кабинете студента. Итоговый тест содержит 20 случайным образом выпадающих тестовых заданий. Каждое оценивается максимально в 0,5 балла, т.о. максимальное общее количество баллов за тест – до 10 баллов.

Пример тестовых вопросов:

1. Какая нотация используется для моделирования информационных процессов? (выберите 1 или более вариантов)

1. IDEF0
2. IDEF3
3. IDEF5
4. UML
5. DFD
6. ISDF

2. Какая графическая нотация используется для моделирования рабочих процессов? (выберите 1 или более вариантов)

1. IDEF0
2. IDEF3
3. IDEF5
4. UML
5. DFD
6. ISDF

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

Критерии оценки результатов итогового тестирования (в баллах)*:*

-0,5 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;

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. Лисяк, В.В. Моделирование информационных систем : учебное пособие / В.В. Лисяк, Н.К. Лисяк ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. – 89 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=561102

2. Душин, В.К. Теоретические основы информационных процессов и систем : учебник : / В.К. Душин. – 5-е изд. – Москва: Дашков и К°, 2018. – 348 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=573118

Дополнительная литература:

3. Антонов, В.Ф. Методы и средства проектирования информационных систем : учебное пособие / В.Ф. Антонов, А.А. Москвитин ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». – Ставрополь : СКФУ, 2016. – 342 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=458663

4. Проектирование информационных систем. Проектный практикум : учебное пособие / А.В. Платёнкин, И.П. Рак, А.В. Терехов, В.Н. Чернышов ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». – Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2015. – 81 с. : ил., схем. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=444966

5. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=480637

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 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.

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 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/1	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 практических занятий: Аудитория № 404. Специализированный кабинет с лабораторным оборудованием. Аудитория № 417. Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами	лабораторные и практические занятия	**Аудитория № 608** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, телевизор TCL-L55P6US. **Аудитория № 404. Специализированный кабинет с лабораторным оборудованием.** Оборудование: учебная мебель, системные блоки\i5-10400 (2.9GHz)\H510M\8Gb\HDD 1Tb\корпус Micro ATX\Win10 Pro, мониторы ЖК 23.8" LG 24MK430H-B (1920x1080, IPS,75 Гц, 5 мс, 1000:1, 250 кд/м2, D-Sub, HDMI, кабель HDMI в комплекте), виртуальный тренажер «Аттестация объекта по требованиям защиты от утечек информации по техническим каналам».

вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации. Аудитория № 507. Лаборатория управления информационной безопасностью. 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/1		**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. **Аудитория № 417. Лаборатория в области технологий обеспечения информационной безопасности и защищенных информационных систем, оснащенная средствами вычислительной техники, сетевым оборудованием, техническими, программными и программно-аппаратными средствами защиты информации и средствами контроля защищенности информации.** Оборудование: учебная мебель, доска, комплект учебного оборудования «Блочное кодирование», комплект учебного оборудования «Основы криптографии», учебно-лабораторный стенд «Аттестация объекта информатизации по требованиям защиты от утечек по каналу побочных ЭМИ» **Аудитория № 507. Лаборатория управления информационной безопасностью.** Оборудование: учебная мебель, доска, мультимедиа, комплекс мониторинга WiFi сетей "Зодиак II", универсальный комплект инструментов для проведения работ по специальным проверкам и специальным обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон".
3. Учебная аудитория для проведения групповых и индивидуальных консультаций: Аудитория № 608 **4. Учебная аудитория для текущего контроля и промежуточной аттестации:** Аудитория № 420. Компьютерный кабинет 450076, Республика Башкортостан, Городской Округ Город Уфа, город Уфа, улица Карла Маркса, дом 3/1	Консультации, текущий контроль, промежуточная аттестация	**Аудитория № 608** Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование, телевизор TCL-L55P6US. **Аудитория № 420. Компьютерный кабинет** Оборудование: учебная мебель, моноблоки Lenovo Thinkcentre A70Z. . **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.

Приложение № 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Моделирование процессов и систем защиты информации
на 4 семестр
очная форма обучения

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (з.е. / часов)	3/108
Учебных часов на контактную работу с преподавателем:	33,2
лекций	16
практических/ семинарских	16
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)	38,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	
Учебных часов на подготовку к экзамену (Контроль)	36

Форма контроля:
Экзамен 4 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. Подходы и методологии моделирования процессов и систем							
1.	1.1. Подходы и методологии моделирования процессов и систем. Системные принципы создания комплексной защиты информации.	1			4	изучение теоретического материала;	практические задания;
2.	1.2. Принципы проектирования СЗИ. Виды показателей эффективности СЗИ. Этапы проектирования СЗИ.	1	2		4	изучение теоретического материала; подготовка докладов	практические задания;
3	1.3. Графические нотации и средства моделирования процессов и проектирования систем защиты информации (СЗИ).	2	2		4	изучение теоретического материала	практические задания; контрольная работа
Раздел 2. Практика моделирования процессов и систем защиты информации							
4	2.1. Моделирование угроз: модель процессов воздействия компьютерных вирусов; модели нарушителя/злоумышленника.	2	2		4	изучение теоретического материала; подготовка к опросу;	практические задания;
5	2.2. Модель представления информации с учетом надежности программно-аппаратных средств.	2	2		4	изучение теоретического материала; подготовка к практическим работам,	практические задания;
6	2.3. Модель управления рисками информационной безопасности.	2	2		4	изучение теоретического материала; подготовка к	практические задания;

						практическим работам,	
7	2.4. Модель процессов сохранения конфиденциальности информации. Модель процессов контроля информации.	2	2		4	изучение теоретического материала; подготовка к практическим работам,	практические задания;
8	2.5. Методы оценки адекватности, устойчивости, чувствительности модели.	2	2		4	изучение теоретического материала; подготовка к практическим работам, курсовое проектирование	практические задания; контрольная работа
9	2.6. Модель системы защиты информации; адаптивность системы информационной безопасности.	2	2		6,8	изучение теоретического материала; подготовка к практическим работам,	практические задания; компьютерный тест.
	Всего часов:	**16**	**16**		**38,8**		