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

Утверждено:
на заседании кафедры
протокол№ 7 от « 18 » февраля 2022 г.
Зав. кафедрой _____ /Исмагилова А.С.

Согласовано:
Председатель УМК института
/ Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина
Моделирование процессов и систем защиты информации
Б1.В.05

программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Профиль подготовки
Организация и технологии защиты информации

Квалификация
специалист

Разработчик (составитель)
к.ф.-м.н., доцент

/И.А. Шагапов

Для приема: 2022 г.

Уфа – 2022

Составитель: доцент Шагапов Илдар Ахняфович

Рабочая программа дисциплины утверждена на заседании кафедры, протокол № 7 от «18» февраля 2022 г.

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета института истории и государственного управления:
_____
_____
_____

Директор _____ А.И. Уразова

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета института истории и государственного управления:
_____
_____
_____

Директор _____ А.И. Уразова

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета института истории и государственного управления:
_____
_____
_____

Директор _____ А.И. Уразова

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета института истории и государственного управления:
_____
_____
_____

Директор _____ А.И. Уразова

Список документов и материалов

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

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

Категория (группа) компетенций (при наличии ОПК)	**Формируемая компетенция (с указанием кода)**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения по дисциплине**
	УК-2 Способен управлять проектом на всех этапах его жизненного цикла	УК 2.1 Знает основы управления проектом на всех этапах его жизненного цикла	Знает основы управления проектом на всех этапах его жизненного цикла
		УК 2.2 Умеет применять основы управления проектом на всех этапах его жизненного цикла	Умеет применять основы управления проектом на всех этапах его жизненного цикла
		УК 2.3 Владеет основными методами управления проектом на всех этапах его жизненного цикла	Владеет основными методами управления проектом на всех этапах его жизненного цикла
	ПК-1 Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей	ПК 1.1 Знает основные требования по защите информации компьютерных систем и сетей	Знает основные требования по защите информации компьютерных систем и сетей
		ПК 1.2 Умеет формировать требования по защите информации компьютерных систем и сетей	Умеет формировать требования по защите информации компьютерных систем и сетей
		ПК 1.3 Владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей	Владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей
	ПК-3 Способен анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации	ПК 3.1 Знает методы анализа защищенности компьютерных систем и эффективности применяемых средств защиты информации	Знает методы анализа защищенности компьютерных систем и эффективности применяемых средств защиты информации
		ПК 3.2 Умеет проводить проверку работоспособности и эффективности применяемых средств защиты информации	Умеет проводить проверку работоспособности и эффективности применяемых средств защиты информации
		ПК 3.3 Владеет основными методами анализа защищенности компьютерных систем и эффективности применяемых средств защиты информации	Владеет основными методами анализа защищенности компьютерных систем и эффективности применяемых средств защиты информации

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Моделирование процессов и систем защиты информации» относится к группе дисциплин вариативной части образовательной программы.

Дисциплина изучается на 5 курсе в 9 семестре.

Целью учебной дисциплины «Моделирование процессов и систем защиты информации» является раскрытие представлений об организационно-правовом обеспечении деятельности государственных и частных структур развитых зарубежных стран по защите информации, что дает возможность сравнить отечественный и зарубежный опыт обеспечения информационной безопасности.

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-2 Способен управлять проектом на всех этапах его жизненного цикла

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Критерии оценивания результатов обучения**			
		«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»
УК 2.1 Знает основы управления проектом на всех этапах его жизненного цикла	Знает основы управления проектом на всех этапах его жизненного цикла	Не знает основы управления проектом на всех этапах его жизненного цикла	Знает некоторые основы управления проектом на всех этапах его жизненного цикла, делает ошибки	Частично знает основы управления проектом на всех этапах его жизненного цикла	Знает основы управления проектом на всех этапах его жизненного цикла
УК 2.2 Умеет применять основы управления проектом на всех этапах его жизненного цикла	Умеет применять основы управления проектом на всех этапах его жизненного цикла	Не умеет применять основы управления проектом на всех этапах его жизненного цикла	Умеет применять некоторые основы управления проектом на всех этапах его жизненного цикла, делает ошибки	Частично умеет применять основы управления проектом на всех этапах его жизненного цикла	Умеет применять основы управления проектом на всех этапах его жизненного цикла
УК 2.3 Владеет основными методами управления проектом на всех этапах его жизненного цикла	Владеет основными методами управления проектом на всех этапах его жизненного цикла	Не владеет основными методами управления проектом на всех этапах его жизненного цикла	Владеет некоторыми методами управления проектом на всех этапах его жизненного цикла, делает ошибки	Частично владеет основными методами управления проектом на всех этапах его жизненного цикла	Владеет основными методами управления проектом на всех этапах его жизненного цикла

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**			
		«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»
ПК 1.1 Знает основные требования по защите информации компьютерных систем и сетей	Знает основные требования по защите информации компьютерных систем и сетей	Не знает основные требования по защите информации компьютерных систем и сетей	Знает некоторые требования по защите информации компьютерных систем и сетей, делает ошибки	Частично знает основные требования по защите информации компьютерных систем и сетей	Знает основные требования по защите информации компьютерных систем и сетей
ПК 1.2 Умеет формировать требования по защите информации компьютерных систем и сетей	Умеет формировать требования по защите информации компьютерных систем и сетей	Не умеет формировать требования по защите информации компьютерных систем и сетей	Умеет формировать некоторые требования по защите информации компьютерных систем и сетей, делает ошибки	Частично умеет формировать требования по защите информации компьютерных систем и сетей	Умеет формировать требования по защите информации компьютерных систем и сетей
ПК 1.3 Владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей	Владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей	Не владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей	Владеет способностью формировать некоторые требования по защите информации и политики безопасности компьютерных систем и сетей, делает ошибки	Частично владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей	Владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей

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**			
		«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»
ПК 3.1 Знает методы анализа защищенности компьютерных систем и эффективности применяемых	Знает методы анализа защищенности компьютерных систем и эффективности применяемых средств	Не знает методы анализа защищенности компьютерных систем и эффективности применяемых средств защиты	Знает некоторые методы анализа защищенности компьютерных систем и эффективности применяемых средств защиты	Частично знает методы анализа защищенности компьютерных систем и эффективности применяемых	Знает методы анализа защищенности компьютерных систем и эффективности применяемых средств

средств защиты информации	защиты информации	информации	информации, делает ошибки	средств защиты информации	защиты информации
ПК 3.2 Умеет проводить проверку работоспособности и эффективности применяемых средств защиты информации	Умеет проводить проверку работоспособности и эффективности применяемых средств защиты информации	Не умеет проводить проверку работоспособности и эффективности применяемых средств защиты информации	Умеет проводить проверку некоторую работоспособности и эффективности применяемых средств защиты информации, делает ошибки	Частично умеет проводить проверку работоспособности и эффективности применяемых средств защиты информации	Умеет проводить проверку работоспособности и эффективности применяемых средств защиты информации
ПК 3.3 Владеет основными методами анализа защищенности компьютерных систем и эффективности применяемых средств защиты информации	Владеет основными методами анализа защищенности компьютерных систем и эффективности применяемых средств защиты информации	Не владеет основными методами анализа защищенности компьютерных систем и эффективности применяемых средств защиты информации	Владеет некоторыми методами анализа защищенности компьютерных систем и эффективности применяемых средств защиты информации, делает ошибки	Частично владеет основными методами анализа защищенности компьютерных систем и эффективности применяемых средств защиты информации	Владеет основными методами анализа защищенности компьютерных систем и эффективности применяемых средств 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

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
УК 2.1 Знает основы управления проектом на всех этапах его жизненного цикла	Знает основы управления проектом на всех этапах его жизненного цикла	Письменная контрольная работа1,2,3,4 Практическое задание 1,2,3,4
УК 2.2 Умеет применять основы управления проектом на всех этапах его жизненного цикла	Умеет применять основы управления проектом на всех этапах его жизненного цикла	Письменная контрольная работа1,2,3,4 Практическое задание 1,2,3,4
УК 2.3 Владеет основными методами управления проектом на всех этапах его жизненного цикла	Владеет основными методами управления проектом на всех этапах его жизненного цикла	Письменная контрольная работа1,2,3,4 Практическое задание 1,2,3,4
ПК 1.1 Знает основные требования по защите информации компьютерных систем и сетей	Знает основные требования по защите информации компьютерных систем и сетей	Письменная контрольная работа1,2,3,4 Практическое задание 1,2,3,4
ПК 1.2 Умеет формировать требования по защите информации компьютерных систем и сетей	Умеет формировать требования по защите информации компьютерных систем и сетей	Письменная контрольная работа1,2,3,4 Практическое задание 1,2,3,4
ПК 1.3 Владеет способностью формировать требования по защите информации и политики безопасности компьютерных	Владеет способностью формировать требования по защите информации и политики безопасности компьютерных систем и сетей	Письменная контрольная работа1,2,3,4 Практическое задание 1,2,3,4

систем и сетей		
ПК 3.1 Знает методы анализа защищенности компьютерных систем и эффективности применяемых средств защиты информации	Знает методы анализа защищенности компьютерных систем и эффективности применяемых средств защиты информации	Письменная контрольная работа1,2,3,4 Практическое задание 1,2,3,4
ПК 3.2 Умеет проводить проверку работоспособности и эффективности применяемых средств защиты информации	Умеет проводить проверку работоспособности и эффективности применяемых средств защиты информации	Письменная контрольная работа1,2,3,4 Практическое задание 1,2,3,4
ПК 3.3 Владеет основными методами анализа защищенности компьютерных систем и эффективности применяемых средств защиты информации	Владеет основными методами анализа защищенности компьютерных систем и эффективности применяемых средств защиты информации	Письменная контрольная работа1,2,3,4 Практическое задание 1,2,3,4

Критериями оценивания при *модульно-рейтинговой системе* являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (*для экзамена:* текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; *для зачета:* текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

(*для экзамена:*

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

Рейтинг – план дисциплины

Моделирование процессов и систем защиты информации

Направление подготовки 10.05.05 БИТвПС

Курс 5, семестр 9

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №1 (реферат)	5	1	0	5
3. Практическая работа №2 (реферат)	5	1	0	5
Рубежный контроль				
1. Письменная контрольная работа №1	7	1	0	7
2. Письменная контрольная работа №2	8	1	0	8
Всего				35
Модуль 2.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
3. Практическая работа №3 (реферат)	5	1	0	5

3. Практическая работа №4 (реферат)	5	1	0	5
Рубежный контроль				
1. Письменная контрольная работа №3	7	1	0	7
2. Письменная контрольная работа №4	8	1	0	8
Всего				35
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Экзамен				30

Комплект практических заданий

Для самостоятельного освоения и/или расширения знаний, умений, владений предусмотрены несколько практических заданий − представление рефератов с последующим обсуждением.

Практическое задание №1

Темы рефератов

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

Критерии и методика оценивания

5 баллов получают, если работа выполнена в полном объеме и изложена грамотным языком в правильной логической последовательности с точным использованием специализированной терминологии; если при этом показано уверенное владение материалом.

4 балла получают за работу, если она выполнена в полном объеме, но имеет некоторые недостатки. К примеру, в работе допущены один-два недочета и/или нет определенной логической последовательности, неточно используется специализированная терминология.

2 балла т получают, если работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформи-

рованность основных умений и навыков (пропорционально количеству недочетов, ошибок, пробелов в знаниях).

Практическое задание №2
Темы рефератов

1. Принципы системного подхода в моделировании.
2. Виды показателей эффективности.
3. Метод обобщенного показателя.
4. Метод целевого программирования.
5. Системный подход к управлению защитой информации. Системные принципы создания комплексной защиты информации.
6. Выбор уровня описания системы в модели. Методология разработки моделей. Алгоритм создания системы комплексной защиты.
7. Модель формирования множества функций защиты информации.

Критерии и методика оценивания

5 баллов получают, если работа выполнена в полном объеме и изложена грамотным языком в правильной логической последовательности с точным использованием специализированной терминологии; если при этом показано уверенное владение материалом.

4 балла получают за работу, если она выполнена в полном объеме, но имеет некоторые недостатки. К примеру, в работе допущены один-два недочета и/или нет определенной логической последовательности, неточно используется специализированная терминология.

2 балла т получают, если работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков (пропорционально количеству недочетов, ошибок, пробелов в знаниях).

Практическое задание №3
Темы рефератов

1. Методы теории игр в информационной безопасности.
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.
7. Вероятностная модель системы контроля доступа к информации.
8. Модель на основе нейронных сетей в задачах защиты информации.
9. Разработка модели управления рисками информационной безопасности.
10. Разработка модели действий инсайдера.

Критерии и методика оценивания

5 баллов получают, если работа выполнена в полном объеме и изложена грамотным языком в правильной логической последовательности с точным использованием специализированной терминологии; если при этом показано уверенное владение материалом.

3 балла получают за работу, если она выполнена в полном объеме, но имеет некоторые недостатки. К примеру, в работе допущены один-два недочета и/или нет определенной логической последовательности, неточно используется специализированная терминология.

2 балла т получают, если работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков (пропорционально количеству недочетов, ошибок,

пробелов в знаниях).

Практическое задание №4

Темы рефератов

1. Методы определения важности требований к процессам и системам защиты информации.
2. Разработка моделей защиты информации.
3. Стратегическое планирование имитационного экспериментов.
4. Тактическое планирование имитационного экспериментов.
5. Оценка качества имитационной модели. Методы оценки адекватности.
6. Методы оценки адекватности, устойчивости, чувствительности модели.
7. Методы оценки чувствительности модели.
8. Калибровка модели.
9. Оценка влияния и взаимосвязи факторов.
10. Разработка модели системы защиты информации.
11. Модель адаптивной системы информационной безопасности.

Критерии и методика оценивания

5 баллов получают, если работа выполнена в полном объеме и изложена грамотным языком в правильной логической последовательности с точным использованием специализированной терминологии; если при этом показано уверенное владение материалом.

4 балла получают за работу, если она выполнена в полном объеме, но имеет некоторые недостатки. К примеру, в работе допущены один-два недочета и/или нет определенной логической последовательности, неточно используется специализированная терминология.

2 балла получают, если работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков (пропорционально количеству недочетов, ошибок, пробелов в знаниях).

Комплект контрольных работ

Письменная контрольная работа №1

Вопросы

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.

Критерии оценки

Выполнен пункт 1 – 1 балл
Выполнены пункты 1-2 – 2 балла
Выполнены пункты 1-3 – 3 балла
Выполнены пункты 1-4 – 4 балла
Выполнены пункты 1-5 – 5 баллов
Выполнены пункты 1-6 –6 баллов
Выполнены пункты 1-7 – 7 баллов
Максимальный балл – 7 баллов

Письменная контрольная работа №2

Вопросы

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.

Критерии оценки

Выполнен пункт 1 – 1 балл
Выполнены пункты 1-2 – 2 балла
Выполнены пункты 1-3 – 3 балла
Выполнены пункты 1-4 – 4 балла
Выполнены пункты 1-5 – 5-6 баллов
Выполнены пункты 1-6 –7 баллов
Выполнены пункты 1-7 – 8 баллов
Максимальный балл – 8 баллов

Письменная контрольная работа №3

Вопросы

1. Стратегическое планирование имитационного экспериментов.
2. Тактическое планирование имитационного экспериментов.
3. Оценка качества имитационной модели. Методы оценки адекватности.

Критерии оценки

Выполнен пункт 1 – 2 балла
Выполнены пункты 1-2 – 4 балла
Выполнены пункты 1-3 – 6 баллов
Максимальный балл – 8 баллов

Письменная контрольная работа №4

Вопросы

1.. Методы оценки устойчивости модели.
2. Методы оценки чувствительности модели.
3. Калибровка модели.
4. Оценка влияния и взаимосвязи факторов.

Критерии оценки

Выполнен пункт 1 – 2 балла
Выполнены пункты 1-2 – 4 балла
Выполнены пункты 1-3 – 6 баллов
Максимальный балл – 8 баллов

Экзаменационные билеты

Структура экзаменационного билета: экзаменационный билет содержит 2 теоретических вопроса.

Перечень вопросов для экзамена:

1. Классификация моделей.
2. Математические модели.
3. Компьютерные модели.
4. Системный подход к защите информации.
5. Системные принципы создания комплексной защиты информации.

6. Выбор уровня описания системы в модели.
7. Этапы моделирования.
8. Виды показателей эффективности.
9. Методы определения важности требований, предъявляемых к системе защиты информации.
10. Выбор уровня описания системы в модели.
11. Алгоритм создания системы комплексной защиты.
12. Методология разработки моделей.
13. Модели процессов в информационном обмене в системах защиты информации.
14. Функции моделирования информационного обмена.
15. Способ перехода от математической модели процесса к цифровой модели: нормировка параметров модели,
16. Способ перехода от математической модели процесса к цифровой модели: задание шага дискретизации .
17. Способ перехода от математической модели процесса к цифровой модели: задание энергетических его характеристики.
18. Определение динамических диапазонов модулируемых процессов.
19. Методы оценки адекватности модели.
20. Методы оценки устойчивости модели.
21. Методы оценки чувствительности модели.
22. Модель представления информации с учетом надежности программно-аппаратных средств.
23. Модель защиты информации.
24. Моделирование процессов защиты информации.
25. Разработка модели управления рисками информационной безопасности.
26. Модель процессов контроля информации.
27. Модель процессов воздействия компьютерных вирусов.
28. Разработка модели действий инсайдера.
29. Разработка модели действий внешнего злоумышленника.
30. Модель процессов сохранения конфиденциальности информации.
31. Модель процессов сохранения целостности информации.
32. Модель процессов сохранения доступности информации.
33. Модель процессов сохранения неотказуемости.
34. Модель синтеза рационального проекта системы защиты информации.
35. Модель адаптивной системы информационной безопасности.
36. Модель злоумышленника.

Образец экзаменационного билета:

…

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

Направление подготовки 10.05.05 БИТвПС

Дисциплина: Моделирование процессов и систем защиты информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Виды показателей эффективности.
2. Разработка модели действий инсайдера.

Зав. кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии оценки (в баллах):

- <u>25-30</u> 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 при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;*

- <u>17-24</u> 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. При выполнении практической части работы допущены несущественные ошибки;*

- <u>10-16</u> *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. Студент не решил задачу или при решении допущены грубые ошибки;*

- <u>0-10</u> 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 при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.*

Темы лекционных занятий

(18 часов)

1. Классификация моделей. Системный подход к защите информации. Системные принципы создания комплексной защиты информации.
2. Выбор уровня описания системы в модели. Этапы моделирования. Виды показателей эффективности. Методы определения важности требований, предъявляемых к системе защиты информации. Выбор уровня описания системы в модели.
3. Алгоритм создания системы комплексной защиты. Методология разработки моделей.
4. Модели процессов в информационном обмене в системах защиты информации.
5. Функции моделирования информационного обмена. Способ перехода от математической модели процесса к цифровой модели: нормировка параметров модели, задание шага дискретизации и энергетических его характеристик. Определение динамических диапазонов модулируемых процессов.
6. Методы оценки адекватности, устойчивости, чувствительности модели. Модель представления информации с учетом надежности программно-аппаратных средств.
7. Разработка модели управления рисками информационной безопасности. Модель процессов контроля информации. Модель процессов воздействия компьютерных вирусов. Разработка модели действий инсайдера.
8. Модель процессов сохранения конфиденциальности информации. Модель синтеза рационального проекта системы защиты информации.
9. Модель адаптивной системы информационной безопасности. Модель злоумышленника.

Темы семинарских занятий

(36 часов)

3. Классификация моделей.
4. Математические модели.
5. Компьютерные модели.
6. Системный подход к защите информации.
7. Системные принципы создания комплексной защиты информации.
8. Выбор уровня описания системы в модели.
9. Этапы моделирования.
10. Виды показателей эффективности.
11. Методы определения важности требований, предъявляемых к системе защиты информации.
12. Выбор уровня описания системы в модели.
13. Алгоритм создания системы комплексной защиты.
14. Методология разработки моделей.
15. Модели процессов в информационном обмене в системах защиты информации.
16. Функции моделирования информационного обмена.
17. Способ перехода от математической модели процесса к цифровой модели: нормировка параметров модели,
18. Способ перехода от математической модели процесса к цифровой модели: задание шага дискретизации .
19. Способ перехода от математической модели процесса к цифровой модели: задание энергетических его характеристики.
20. Определение динамических диапазонов модулируемых процессов.
21. Методы оценки адекватности модели.
22. Методы оценки устойчивости модели.
23. Методы оценки чувствительности модели.
24. Модель представления информации с учетом надежности программно-аппаратных средств.
25. Модель защиты информации.
26. Моделирование процессов защиты информации.
27. Разработка модели управления рисками информационной безопасности.
28. Модель процессов контроля информации.
29. Модель процессов воздействия компьютерных вирусов.
30. Разработка модели действий инсайдера.
31. Разработка модели действий внешнего злоумышленника.
32. Модель процессов сохранения конфиденциальности информации.
33. Модель процессов сохранения целостности информации.
34. Модель процессов сохранения доступности информации.
35. Модель процессов сохранения неотказуемости.
36. Модель синтеза рационального проекта системы защиты информации.
37. Модель адаптивной системы информационной безопасности.
38. Модель злоумышленника.

Критерии оценки (в баллах) *(должны строго соответствовать рейтинг плану по макс. и мин. колич. баллов и только для тех, кто учится с использованием модульно-рейтинговой системы обучения и оценки успеваемости студентов):*

- *0,5 баллов выставляется студенту, если выполнил задание на 100%*
- *0,4 баллов выставляется студенту, если выполнил задание на 75%*
- *0,3 баллов выставляется студенту, если выполнил задание на 50%*
- *0 баллов выставляется студенту, если не выполнил задание*

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 : [16+] / 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

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	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения Реквизиты подтверждающего документа
1	2	3
1. Учебная аудитория для проведения занятий лекционного типа: Аудитория № 515. 450076, Республика Башкортостан, г. Уфа, ул. Карла Маркса, д. 3, корп. 4 (6 этаж № 5).	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, комер встраиваемый в кафедру INTEL-Corei3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/ThermaltakeVL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром.	Windows 8 Russian Windows Professional 8 Russian Upgrade. Договор №104 от 17.06.2013 г. Лицензии бессрочные. Microsoft Office Standard 2013 Russian. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
2. Учебная аудитория для проведения занятий семинарского типа:	Аудитория № 608. Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование	
3. Учебная аудитория для проведения групповых и индивидуальных консультаций: Аудитория № 608. 450076, Республика Башкортостан, г. Уфа, ул. Карла Маркса, д. 3, корп. 4 (6 этаж № 49).	Аудитория № 608. Оборудование: учебная мебель, доска, мобильное мультимедийное оборудование	
4. Учебная аудитория для текущего контроля и промежуточной аттестации: Аудитория № 420. Компьютерный класс 450076,	Аудитория № 420. Компьютерный класс Оборудование: учебная мебель, моноблоки стационарные 15 шт., мобильное мультимедийное оборудование, переносной экран.	

Республика Башкортостан, г. Уфа, ул. Карла Маркса, д. 3, корп. 4 (4 этаж № 23).		
5. Помещения для самостоятельной работы: Аудитория № 402 (читальный зал) 450076, Республика Башкортостан, г. Уфа, ул. Карла Маркса, д. 3, корп. 4. (4 этаж № 5). Аудитория № 613 450076, Республика Башкортостан, г. Уфа, ул. Карла Маркса, д. 3, корп. 4. (6 этаж № 4).	Аудитория № 402 (читальный зал) Оборудование: Учебная мебель, стенд по пожарной безопасности, моноблоки стационарные – 5 шт. с возможностью подключения к сети Интернет и доступа в электронную информационно-образовательную среду, принтер – 1 шт., сканер – 1 шт. Аудитория № 613 Оборудование: учебная мебель, доска, моноблок стационарный – 12 шт. с возможностью подключения к сети Интернет и доступа в электронную информационно-образовательную среду.	
6. Помещение для хранения и профилактического обслуживания учебного оборудования: Аудитория № 523 450076, Республика Башкортостан, г. Уфа, ул. Карла Маркса, д. 3, корп. 4. (5 этаж № 14).	Аудитория № 523 Оборудование: стол, стул, шкаф-стеллаж, мобильное мультимедийное оборудование – проектор, ноутбук, экран переносной	

Приложение 1

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

Содержание рабочей программы
дисциплины

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	55
лекций	18
практических/ семинарских	36
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	7.8
Учебных часов на подготовку к экзмену	45

Форма контроля:
экзамен 9 семестр

№	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	7	8
1	Классификация моделей. Системный подход к защите информации. Системные принципы создания комплексной защиты информации.	2	4		0	Самостоятельное изучение рекомендуемых источников и материалов	Письменная контрольная работа, реферат
2	Выбор уровня описания системы в модели. Этапы моделирования. Виды показателей эффективности. Методы определения важности требований, предъявляемых к системе защиты информации. Выбор уровня описания системы в модели.	2	4		1	Самостоятельное изучение рекомендуемых источников и материалов	Письменная контрольная работа, реферат
3	Алгоритм создания системы комплексной защиты. Методология разработки моделей.	2	4		0,8	Самостоятельное изучение рекомендуемых источников и материалов	Письменная контрольная работа, реферат
4	Модели процессов в информационном обмене в системах защиты информации.	2	4		1	Самостоятельное изучение рекомендуемых источников и материалов	Письменная контрольная работа, реферат
5	Функции моделирования информационного обмена. Способ перехода от математической модели процесса к цифровой модели: нормировка параметров модели, задание шага дискретизации и энергетических его характеристик. Определение динамических диапазонов модулируемых процессов.	2	4		1	Самостоятельное изучение рекомендуемых источников и материалов	Письменная контрольная работа, реферат
6	Методы оценки адекватности, устойчивости, чувствительности модели. Модель представления информации с учетом надежности программно-аппаратных средств.	2	4		1	Самостоятельное изучение рекомендуемых источников и материалов	Письменная контрольная работа, реферат
7	Разработка модели управления	2	4		1	Самостоятельное изучение реко-	Письменная контрольная

	рисками информационной безопасности. Модель процессов контроля информации. Модель процессов воздействия компьютерных вирусов. Разработка модели действий инсайдера.					мендуемых источников и материалов	работа, реферат
8	Модель процессов сохранения конфиденциальности информации. Модель синтеза рационального проекта системы защиты информации.	2	4		1	Самостоятельное изучение рекомендуемых источников и материалов	Письменная контрольная работа, реферат
9	Модель адаптивной системы информационной безопасности. Модель злоумышленника.	2	4		1	Самостоятельное изучение рекомендуемых источников и материалов	Письменная контрольная работа, реферат
	Итого	18	36		7.8		72