


МИНОБРНАУКИ РОССИИ
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 (МОДУЛЯ)

Дисциплина
Основы моделирования процессов и систем защиты информации
Обязательная часть
программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

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

Квалификация
бакалавр

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



/И.А. Шагапов

Для приема: 2021 г.

Уфа – 2021

Составитель: доцент Шагапов Илдар Ахняфович

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

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций	4
2. Цель и место дисциплины в структуре образовательной программы	5
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)	5
4. Фонд оценочных средств по дисциплине	5
4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине	5
4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине	7
5. Учебно-методическое и информационное обеспечение дисциплины	14
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	14
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы	15
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	15

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
	ОПК-7 Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-7.7. Знать современные тенденции развития математического аппарата и информационных технологий для решения задач профессиональной деятельности.	Знает современные тенденции развития математического аппарата и информационных технологий для решения задач профессиональной деятельности.
		ОПК-7.8. Уметь разрабатывать и анализировать математические модели и использовать достижения современных информационных технологий, измерительной и вычислительной техники для решения профессиональных задач.	Умеет разрабатывать и анализировать математические модели и использовать достижения современных информационных технологий, измерительной и вычислительной техники для решения профессиональных задач.
		ОПК-7.9. Владеть современным математическим и инструментальным аппаратом для решения профессиональных задач.	Владеет современным математическим и инструментальным аппаратом для решения профессиональных задач.
	ОПК-2.2 Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	ОПК 2.2.1 Знать основы формирования предложений по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	Знает основы формирования предложений по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы
		ОПК 2.2.2 Уметь формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	Умеет формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы
		ОПК 2.2.3 Владеть основами формирования предложений по оптимизации структуры и функциональных процессов объекта защиты и его информационных	Владеет основами формирования предложений по оптимизации структуры и функциональных процессов объекта защиты и его информационных

		ных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	щих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы
--	--	---	--

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Основы моделирования процессов и систем защиты информации» относится к группе дисциплин основной части образовательной программы.

Дисциплина изучается на 3 курсе в 6 семестре.

Целью учебной дисциплины «Основы моделирования процессов и систем защиты информации» является дать студентам необходимые знания, умения и навыки использования современных методов и средств создания и эксплуатации моделей процессов и систем защиты информации.

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 соотношенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине

ОПК-7 Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения (зачет)	
		«Незачтено»	«Зачтено»
ОПК-7.7. Знать современные тенденции развития математического аппарата и информационных технологий для решения задач профессиональной деятельности.	Знает современные тенденции развития математического аппарата и информационных технологий для решения задач профессиональной деятельности.	Не знает современные тенденции развития математического аппарата и информационных технологий для решения задач профессиональной деятельности.	Знает современные тенденции развития математического аппарата и информационных технологий для решения задач профессиональной деятельности.
ОПК-7.8. Уметь разрабатывать и анализировать математические модели и использовать достижения современных информационных технологий, измерительной и вычислительной техники для решения профессиональных задач.	Умеет разрабатывать и анализировать математические модели и использовать достижения современных информационных технологий, измерительной и вычислительной техники для решения профессиональных задач.	Не умеет разрабатывать и анализировать математические модели и использовать достижения современных информационных технологий, измерительной и вычислительной техники для решения профессиональных задач.	Умеет разрабатывать и анализировать математические модели и использовать достижения современных информационных технологий, измерительной и вычислительной техники для решения профессиональных задач.
ОПК-7.9. Вла-	Владеет современ-	Не владеет современным матема-	Владеет современным ма-

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
<p>ОПК-7.7. Знать современные тенденции развития математического аппарата и информационных технологий для решения задач профессиональной деятельности.</p> <p>ОПК-7.8. Уметь разрабатывать и анализировать математические модели и использовать достижения современных информационных технологий, измерительной и вычислительной техники для решения профессиональных задач.</p> <p>ОПК-7.9. Владеть современным математическим и инструментальным аппаратом для решения профессиональных задач.</p>	<p>Знает современные тенденции развития математического аппарата и информационных технологий для решения задач профессиональной деятельности.</p>	<p>Письменная контрольная работа 1,2,3,4</p> <p>Практическое задание 1,2,3,4</p>
	<p>Умеет разрабатывать и анализировать математические модели и использовать достижения современных информационных технологий, измерительной и вычислительной техники для решения профессиональных задач.</p>	<p>Письменная контрольная работа 1,2,3,4</p> <p>Практическое задание 1,2,3,4</p>
	<p>Владеет современным математическим и инструментальным аппаратом для решения профессиональных задач.</p>	<p>Письменная контрольная работа 1,2,3,4</p> <p>Практическое задание 1,2,3,4</p>

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
<p>ОПК 2.2.1 Знать основы формирования предложений по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы</p> <p>ОПК 2.2.2 Уметь формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы</p> <p>ОПК 2.2.3 Владеть основами формирования предложений по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы</p>	<p>Знает основы формирования предложений по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы</p>	<p>Письменная контрольная работа 1,2,3,4</p> <p>Практическое задание 1,2,3,4</p>
	<p>Умеет формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы</p>	<p>Письменная контрольная работа 1,2,3,4</p> <p>Практическое задание 1,2,3,4</p>
	<p>Владеет основами формирования предложений по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы</p>	<p>Письменная контрольная работа 1,2,3,4</p> <p>Практическое задание 1,2,3,4</p>

Критериями оценивания при *модульно-рейтинговой системе* являются баллы, кото-

рые 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 зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
не зачтено – от 0 до 59 рейтинговых баллов)

Рейтинг – план дисциплины

Основы моделирования процессов и систем защиты информации

Направление подготовки 10.03.01 ИБ

Курс 3, семестр 6

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)	10	1	0	10
3. Практическая работа №2 (реферат)	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №1	10	1	0	10
2. Письменная контрольная работа №2	10	1	0	10
Всего				50
Модуль 2.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
3. Практическая работа №3 (реферат)	10	1	0	10
3. Практическая работа №4 (реферат)	10	1	0	10
Рубежный контроль				
1. Письменная контрольная работа №3	10	1	0	10
2. Письменная контрольная работа №4	10	1	0	10
Всего				50
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				
Зачет				

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

7-5 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.

4-3 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.

2-1 балл 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 №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

10-8 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.

7-5 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.

4-1 балл 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

10-8 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.

7-5 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.

4-1 балл 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. Tактическое 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

10-8 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.

7-5 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.

4-1 балл 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 – 3 балла
Выполнены пункты 1-2 – 4-5 баллов
Выполнены пункты 1-3 – 6 баллов
Выполнены пункты 1-4 – 7 баллов
Выполнены пункты 1-5 – 8 баллов
Выполнены пункты 1-6 – 9 баллов
Выполнены пункты 1-7 – 10 баллов
Максимальный балл – 10 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 – 3 балла
Выполнены пункты 1-2 – 4-5 баллов
Выполнены пункты 1-3 – 6 баллов
Выполнены пункты 1-4 – 7 баллов
Выполнены пункты 1-5 – 8 баллов

Выполнены пункты 1-6 – 9 баллов
Выполнены пункты 1-7 – 10 баллов
Максимальный балл – 10 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 – 6 баллов
Выполнены пункты 1-3 – 10 баллов
Максимальный балл – 10 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 – 2 балла
Выполнены пункты 1-3 – 6 баллов
Выполнены пункты 1-4 – 10 баллов
Максимальный балл – 10 баллов

Перечень вопросов для зачета:

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.

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

Шкалы оценивания:

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

не зачтено – от 0 до 59 рейтинговых баллов).

Темы лекционных занятий

(16 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. Модель адаптивной системы информационной безопасности. Модель злоумышленника.

Темы семинарских занятий

(32 часа)

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. Модель процессов сохранения конфиденциальности информации.
30. Модель синтеза рационального проекта системы защиты информации.
31. Модель адаптивной системы информационной безопасности.
32. Модель злоумышленника.

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. Справочная правовая система «КонсультантПлюс» – <http://www.consultant-plus.ru>.
2. Электронная библиотечная система «Университетская библиотека онлайн» – <https://biblioclub.ru>.
3. Электронная библиотечная система издательства «Лань» – <https://e.lanbook.com/>
4. Электронный каталог Библиотеки БашГУ – <http://www.bashlib.ru/catalog/>
5. www.fstec.ru – сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. <http://window.edu.ru/> – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. <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);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www.edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. 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.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
1. учебная аудитория для проведения занятий лекционного типа: аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гу-	Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	Аудитория № 403 Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. Аудитория № 405 Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт.,	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.

<p>манитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус).</p> <p>2. учебная аудитория для проведения лабораторных работ: Лаборатория полигон технической защиты информации № 508 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (гуманитарный корпус).</p> <p>3. учебная аудитория для проведения занятий семинарского типа: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус).</p> <p>4. учебная аудитория для проведения групповых и индивидуальных консультаций: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).</p> <p>5. учебная аудитория для текущего контроля и промежуточной аттестации: аудитория № 403</p>		<p>Ком-ер встраиваемый в кафедру INTEL-Corei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMIC-MPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт.</p> <p>Аудитория № 413 Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p>Аудитория № 415 Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p>Аудитория № 416 Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.</p> <p>Аудитория № 418 Учебная мебель, доска, Экран настенный Lumien Master Piktura 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт.</p> <p>Аудитория № 419 Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт.</p> <p>Аудитория № 515 Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с попитром.</p> <p>Аудитория № 516 Учебная мебель, доска, кресла секци-</p>	<p>2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.</p> <p>3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License. Лицензии бессрочные.</p>
---	--	---	---

<p>(гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).</p> <p>6. помещения для самостоятельной работы: читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус).</p> <p>7.помещение для хранения и профилактического обслуживания учебного оборудования: аудитория № 523 (гуманитарный корпус).</p>		<p>онные последующих рядов с проектором, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.</p> <p>Аудитория № 509 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 608 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 609 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 610 Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м.</p> <p>Аудитория № 613 Учебная мебель, доска, моноблок стационарный – 15 шт.</p> <p>Компьютерный класс аудитория № 420 Учебная мебель, моноблоки стационарные 15 шт.</p> <p>Компьютерный класс аудитория № 404 Учебная мебель, компьютеры -15 штук.</p> <p>Аудитория 402 читальный зал библиотеки Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные.</p> <p>Лаборатория полигон технической защиты информации № 508 Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технической защиты информации, комплекс мониторинга WiFi сетей "Зодиак II", универсальный ком-плект 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".</p> <p>Аудитория № 523 Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.</p>	
---	--	---	--

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)	2 ЗЕТ / 72 часа
Учебных часов на контактную работу с преподавателем:	48
лекций	16
практических/ семинарских	32
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	24
Учебных часов на подготовку к зачету	

Форма контроля:
 зачет 6 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		3	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		3	Самостоятельное изучение рекомендуемых источников и материалов	Письменная контрольная работа, реферат
3	Алгоритм создания системы комплексной защиты. Методология разработки моделей.	2	4		3	Самостоятельное изучение рекомендуемых источников и материалов	Письменная контрольная работа, реферат
4	Модели процессов в информационном обмене в системах защиты информации.	2	4		3	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		3	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		3	Самостоятельное изучение рекомендуемых источников и материалов	Письменная контрольная работа, реферат

7	Разработка модели управления рисками информационной безопасности. Модель процессов контроля информации. Модель процессов воздействия компьютерных вирусов. Разработка модели действий инсайдера.	2	4		3	Самостоятельное изучение рекомендуемых источников и материалов	Письменная контрольная работа, реферат
8	Модель процессов сохранения конфиденциальности информации. Модель синтеза рационального проекта системы защиты информации. Модель адаптивной системы информационной безопасности. Модель злоумышленника.	2	4		3	Самостоятельное изучение рекомендуемых источников и материалов	Письменная контрольная работа, реферат
	Итого	16	32		24		72

