

Подписано электронной подписью:

Вержицкий Данил Григорьевич

Должность: Директор КГПИ ФГБОУ ВО «КемГУ»

Дата и время: 2024-02-21 00:00:00

471086fad29a3b30e244c728abc3661ab35c9d50210dcf0e75e03a5b6fdf6436

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кемеровский государственный университет»

Новокузнецкий институт (филиал)

федерального государственного бюджетного образовательного учреждения
высшего образования

«Кемеровский государственный университет»

Факультет информационных технологий

Кафедра информатики и вычислительной техники им. В.К. Буторина



Т.В. Бурнышева

« 27 » февраля 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.13 Информационная безопасность автоматизированных систем обработки информации и управления

Направление подготовки

09.03.01 Информатика и вычислительная техника

Направленность (профиль) подготовки

Автоматизированные системы обработки информации и управления

Уровень бакалавриата

Программа

Академический бакалавриат

Квалификация выпускника

Бакалавр

Форма обучения

очная, очно-заочная, заочная

Год набора 2018

Новокузнецк 2018

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы	3
2. Место дисциплины в структуре ООП бакалавриата	4
3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся	6
3.1. Объём дисциплины (модуля) по видам учебных занятий (в часах)	6
4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.....	7
4.1. Разделы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах)	7
4.2 Содержание дисциплины, структурированное по темам	9
Построение матрицы рисков для выбранного предприятия.	12
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	13
6. Фонд оценочных средств для проведения промежуточной аттестации	14
6.1. Паспорт фонда оценочных средств по дисциплине.....	14
6.2 Типовые контрольные задания или иные материалы.....	16
6.3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций.....	21
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	22
8. Перечень ресурсов информационно-телекоммуникационной сети «интернет», необходимых для освоения дисциплины	23
9. Методические указания для обучающихся по освоению дисциплины	24
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем	25
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	26
12. Иные сведения и (или) материалы	27
12.1. Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине	27

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Целью курса является приобретение студентами теоретических знаний и практических навыков обеспечения различных методов защиты информационных систем.

Данная дисциплина направлена на формирование следующих *компетенций*:

- ОПК-5 (способностью устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем)
- ОПК-5 (способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности)

В результате освоения ООП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине (модулю):

Код компетенции по ФГОС	Результаты освоения ООП <i>Содержание</i>	Перечень планируемых результатов обучения по дисциплине
ОПК-5	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: - виды угроз, возникающие в процессе информационной деятельности - методы и средства обеспечения информационной безопасности объектов профессиональной деятельности Уметь: - выявлять угрозы информационной безопасности; - анализировать и выбирать методы и средства обеспечения информационной безопасности. Владеть: - методами и средствами обеспечения информационной безопасности объектов профессиональной деятельности.

2. Место дисциплины в структуре ООП бакалавриата

Дисциплина «Защита информации» относится к обязательным дисциплинам вариативной части блока Б1 (Б1.В.ОД.16).

Дисциплина изучается на 3 курсе в 6 семестре при очной форме обучения и на 4 курсе в 7 семестре при очно-заочной форме обучения.

Дисциплина «Методы и средства защиты информации» участвует в формировании компетенции ОПК-5 совместно с дисциплинами, представленными в таблице 2

Таблица 2 – Структурно-логическая схема формирования компетенций

Компетенция	Предыдущие дисциплины	Данная дисциплина	Последующие дисциплины
ОПК-5	- Информатика (1 сем.) - Введение в специальность (1 сем.) - Математика (1-2 сем.) - Дискретная математика (2-3 сем.) - Теория вероятностей и математическая статистика (3 сем.) - Физика (3-4 сем.)	Методы и средства защиты информации	- Учебная практика - Итоговая государственная аттестация

Таблица 3 – Входные знания, умения, навыки, необходимые для изучения данной дисциплины

Знания	Умения	Навыки
- дискретности и непрерывности в природе и обществе; - основные положения теории информации и кодирования; - виды, формы и способы представления и преобразования данных; - представление данных в ПК; - состав и структуру персональных компьютеров; - иметь представление об алгоритмических языках программирования.	- применять языки программирования для решения математических задач; - выполнять арифметические и логические операции над числами в различных системах счисления; - выявлять формы и способы представления данных.	- применение информационных технологий для решения математических задач; - использование различных систем счисления; - использовать универсальные технологии подключения к базам данных; - о передовых технологиях Microsoft для работы с базами данных.

Таблица 4 – Deskрипторные характеристики компетенций, формируемые в результате освоения дисциплины

Код компетенции	Формируемые компетенции	Deskрипторные характеристики компетенций
ОПК-5	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: - виды угроз, возникающие в процессе информационной деятельности - методы и средства обеспечения информационной безопасности объектов профессиональной деятельности Уметь: - выявлять угрозы информационной безопасности; - анализировать и выбирать методы и средства обеспечения информационной безопасности. Владеть: - методами и средствами обеспечения информационной безопасности объектов профессиональной деятельности.

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины (модуля) составляет 3 (три) зачетные единицы (ЗЕТ), 108 (сто восемь) академических часов.

3.1. Объем дисциплины (модуля) по видам учебных занятий (в часах)

Объём дисциплины	Всего часов	
	для очной формы обучения	для очно-заочной формы обучения
Общая трудоемкость дисциплины	108	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	40	20
Аудиторная работа (всего):	40	20
в т. числе:		
Лекции	20	10
Семинары, практические занятия	-	
Практикумы	-	
Лабораторные работы	20	10
Внеаудиторная работа (всего):	-	-
В том числе, индивидуальная работа обучающихся с преподавателем:	-	-
Курсовое проектирование	-	-
Контрольная работа	-	-
Творческая работа (эссе)	-	-
Самостоятельная работа обучающихся (всего)	68	88
Вид промежуточной аттестации обучающегося – зачет с оценкой	зачет	зачет

4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах)

для очной формы обучения

№ п/п	Раздел дисциплины	Общая трудоемкость (<i>часов</i>)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоя- тельная работа обучаю- щихся	
		всего	лек- ции	семинары, практичес- кие занятия		
1.	Введение в предмет. Угрозы информационной безопасности	9	2	2	5	Устный доклад; отчет по лабора- торной работе.
2.	Основные понятия теории информационной безопасности	9	2	2	5	Устный доклад; Отчет по лабора- торной работе.
3.	Программно- технические методы защиты	24	4	4	16	Устный доклад; Отчет по лабораторной работе.
4.	Криптографические методы защиты	24	4	4	16	Устный доклад; Отчет по лабора- торной работе.
5.	Организационно правовые методы информационной безопасности	9	2	2	5	Устный доклад; Отчет по лабораторной работе.
6.	Роль стандартов в обеспечении информационной безопасности	9	2	2	5	Устный доклад; Отчет по лабораторной работе.
7.	Технологии построения защищенных систем	24	4	4	16	Устный доклад; Отчет по лабораторной работе
Форма контроля						Зачет
ИТОГО		108	20	68	68	

для очно-заочной формы обучения

№ п/п	Раздел дисциплины	Общая трудоемкость (<i>часов</i>)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоя- тельная работа обучаю- щихся	
		всего	лек- ции	семинары, практичес- кие занятия		
1.	Введение в предмет. Угрозы информационной безопасности	9	1	1	7	Устный доклад; отчет по лабора- торной работе.
2.	Основные понятия теории информационной безопасности	9	1	1	7	Устный доклад; Отчет по лабора- торной работе.
3.	Программно- технические методы защиты	24	2	2	20	Устный доклад; Отчет по лабораторной работе.
4.	Криптографические методы защиты	24	2	2	20	Устный доклад; Отчет по лабора- торной работе.
5.	Организационно правовые методы информационной безопасности	9	1	1	7	Устный доклад; Отчет по лабораторной работе.
6.	Роль стандартов в обеспечении информационной безопасности	9	1	1	7	Устный доклад; Отчет по лабораторной работе.
7.	Технологии построения защищенных систем	24	2	2	20	Устный доклад; Отчет по лабораторной работе
Форма контроля						Зачет
ИТОГО		108	10	10	88	

4.2 Содержание дисциплины, структурированное по темам

Содержание лекционного курса

№ п/п	Наименование раздела дисциплины	Содержание
1	Введение в предмет. Угрозы информационной безопасности	Понятие информационной безопасности и защищенной системы. Международные стандарты информационного обмена. Понятие угрозы. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные задачи обеспечения защиты информации. Основные методы и средства защиты информационных систем. Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.). Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности. Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.
2	Основные понятия теории информационной безопасности	Основные положения теории информационной безопасности информационных систем. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Формальные модели безопасности их значение для построения защищенных информационных систем. Понятие доступа к данным и мониторинга безопасности. Функции мониторинга безопасности. Понятие политики безопасности информационных систем. Разработка и реализация политики безопасности. Управление доступом к данным. Основные типы политики безопасности управления доступом к данным: дискреционная и мандатная политика безопасности. Анализ способов нарушений безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
3	Программно-технические методы защиты	Общее представление о структуре защищенной информационной системы. Особенности современных информационных систем, факторы влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности.

№ п/п	Наименование раздела дисциплины	Содержание
		Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей. Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом. Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита. Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах. Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.
4	Криптографические методы защиты	Методы криптографии. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации. Причины нарушения безопасности информации при ее обработке СКЗИ (утечки информации по техническому каналу, неисправности в элементах СКЗИ, работа совместно с другими программами). Использование криптографических средств для решения задач идентификация и аутентификация. Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов информационной системы. Контроль за целостностью информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.
5	Организационно правовые методы информационной безопасности	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной

№ п/п	Наименование раздела дисциплины	Содержание
		безопасности.
6	Роль стандартов в обеспечении информационной безопасности	Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”). Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности. Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности. Руководящие документы Гостехкомиссии России. Структура требований безопасности. Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации. Показатели защищенности средств вычислительной техники от НСД. Классы защищенности автоматизированных систем. Международные стандарты информационной безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Единые критерии»). Основные положения Единых критериев. Функциональные требования и требования доверия. Понятие Профиля защиты и Проекта защиты.
7	Технологии построения защищенных систем	Использование защищенных компьютерных систем. Общие принципы построения защищенных систем. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Исследование корректности реализации и верификации автоматизированных систем. Спецификация требований предъявляемых к системе. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности

Содержание лабораторных занятий

№	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Введение в предмет. Угрозы информационной безопасности	Построение матрицы рисков для выбранного предприятия.
2	Основные понятия теории информационной безопасности	Знакомство с основными направлениями работ в рамках федеральной программы «Электронная Россия», а также со сведениями о порядке использования и действующих алгоритмах постановки ЭЦП.
3	Программно-технические методы защиты	Исследование защиты с применением пароля, а также исследование методов противодействия атакам на пароль.
4	Криптографические методы защиты	Методы современной криптографии на примере программирования одного из предложенных алгоритмов.
5	Организационно правовые методы информационной безопасности	Проведение анализ способов нарушений безопасности на прим.
6	Роль стандартов в обеспечении информационной безопасности	Изучение логики работы и формы предоставления информации сетевыми анализаторами; овладение приемами анализа сетевого трафика; получение базовых знаний для обнаружения и организации сетевых атак.
7	Технологии построения защищенных систем	Составление документа «Политика безопасности»

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Общий объем самостоятельной работы студентов по дисциплине включает аудиторную и внеаудиторную самостоятельную работу студентов в течение семестра.

Аудиторная самостоятельная работа осуществляется в форме выполнения тестовых заданий по дисциплине. Аудиторная самостоятельная работа обеспечена базой тестовых материалов, которая включает два варианта, в каждом из которых 30 заданий. Тестовые материалы хранятся в распечатанном виде на кафедре информационных систем и управления в закрытом для студентов доступе в папке «Контрольно-измерительные материалы».

Внеаудиторная самостоятельная работа осуществляется в форме:

- подготовки к устным докладам. Вопросы для устного опроса приведены в п. 6.2.2.

Для обеспечения самостоятельной работы обучающихся по дисциплине разработан учебно-методический комплекс (УМК), находящийся в свободном доступе локальной сети Вуза по адресу: (\\led\litera\ ФИТ\ Кафедра Информатики и вычислительной техники\УМК).

В состав УМК включены: краткий конспект лекций, задания для выполнения лабораторных работ, методические рекомендации для обучающихся и преподавателей.

6. Фонд оценочных средств для проведения промежуточной аттестации

6.1. Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции / ее формулировка	Наименование оценочного средства
1	Введение в предмет. Угрозы информационной безопасности	ОПК-5 Знать: - методы и средства обеспечения безопасности при инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем Владеть: - методами и средствами обеспечения безопасности при инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем	Вопросы к экзамену № 1-5. Отчет по лабораторной работе.
2	Основные понятия теории информационной безопасности	ОПК-5 Знать: - методы и средства обеспечения безопасности при инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем Владеть: - методами и средствами обеспечения безопасности при инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем	Вопросы к экзамену № 6- 11. Отчет по лабораторной работе.
3	Программно-технические методы защиты	ОПК-5 Владеть: - методами и средствами обеспечения безопасности при инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем	Вопросы к экзамену № 12-19. Отчет по лабораторной работе.
		ОПК-5 Знать: - виды угроз, возникающие в процессе информационной деятельности - методы и средства обеспечения информационной безопасности объектов профессиональной деятельности	
4	Криптографические методы защиты	ОПК-5 Уметь:	Вопросы к экзамену

		- выявлять угрозы информационной безопасности; - анализировать и выбирать методы и средства обеспечения информационной безопасности Владеть: - методами и средствами обеспечения информационной безопасности	№ 20-24. Отчет по лабораторной работе.
5	Организационно правовые методы информационной безопасности	ОПК-5 Владеть: - методами и средствами обеспечения безопасности при инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем	Вопросы к экзамену № 25-30. Отчет по лабораторной работе.
6	Роль стандартов в обеспечении информационной безопасности	ОПК-5 Знать: - виды угроз, возникающие в процессе информационной деятельности - методы и средства обеспечения информационной безопасности объектов профессиональной деятельности	Вопросы к экзамену № 31-36. Отчет по лабораторной работе.
7	Технологии построения защищенных систем	ОПК-5 Уметь: - выявлять угрозы информационной безопасности; - анализировать и выбирать методы и средства обеспечения информационной безопасности Владеть: - методами и средствами обеспечения информационной безопасности	Вопросы к экзамену № 37-41. Отчет по лабораторной работе.

6.2 Типовые контрольные задания или иные материалы

6.2.1 Экзамен

Экзаменационные билеты для проведения экзамена в 7 семестре формируются на основе теоретических вопросов и практических заданий. Билет содержит два теоретических вопроса и одно практическое задание.

а) Типовые вопросы к экзамену

Тема 1. Введение в предмет. Угрозы информационной безопасности.

1. Что называется информационной безопасностью?
2. Какие данные называются критическими?
3. Какие вы знаете признаки компьютерных преступлений в интернет технологиях и какие основные технологии, и методы используются при совершении компьютерных преступлений?
4. Какие четыре уровня защиты компьютерных (интернет технологий) и информационных ресурсов вы можете назвать?
5. Перечислите признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности?

Тема 2. Основные понятия теории информационной безопасности.

6. Перечислите меры защиты информационной безопасности?
7. Какие меры предпринимают по защите целостности информации?
8. Какие меры предпринимают по защите системных программ?
9. Дублирование информации и его классы.
10. Перечислите позиции административного уровня.
11. Назовите цель ОНРВ и его основные положения?

Тема 3. Программно-технические методы защиты.

12. Что такое межсетевой экран и какая у него роль в защите.
13. Законодательная основа информационной безопасности, статьи и пр.
14. Что такое политика безопасности на административном уровне?
15. Основные принципы защиты информации на административном уровне?
16. Средства Разграничения доступа.
17. Что такое CGI процедуры, их назначения?
18. Чем опасна программа, полученная из ненадежного источника, какие вы знаете средства контроля над такими программами?
19. Как осуществляется защита WEB-серверов?

Тема 4. Криптографические методы защиты.

20. Криптография и криптоанализ. Назначение криптографии.
21. Перечислите известные алгоритмы шифрования. Цифровые деньги и их характеристики.
22. Симметричная и асимметричная методология шифрования.
23. Криптографические средства защиты.
24. Квантовая криптография и ККС.

Тема 5. Организационно-правовые методы информационной безопасности.

25. Чем определяется концепция обеспечения безопасности АСОИ.
26. В чем состоит избирательная политика безопасности способом управления доступом.
27. Организационные меры безопасности АСОИ.
28. Матрица доступа в АСОИ.
29. Полномочное управление доступом.
30. Избирательное управление доступом.

Тема 6. Роль стандартов в обеспечении информационной безопасности.

31. Что такое универсальная операционная система?
32. Что такое компьютерный вирус.
33. Полиморфные вирусы.
34. Суррогатные платежные средства.
35. Файловые вирусы и алгоритм их работы.
36. Особенность макровирусов.

Тема 7. Технологии построения защищенных систем.

37. Полномочное управление доступом.
38. Избирательное управление доступом.
39. Отказоустойчивые компьютерные системы.
40. Что вы понимаете под технологией RAID.
41. Методы дублирования информации.

б) Типовые практические задания на экзамен

Задание 1. Для одноалфавитного метода с задаваемым смещением выполнить шифрование с произвольным смещением.

Задание 2. Для одноалфавитного метода с задаваемым смещением выполнить дешифрование зашифрованный шифром Цезаря текст.

Задание 3. Проверить на простоту два произвольных целых числа разрядностью 5.

Задание 4. Задан интервал вида $[x, x + L]$. Вычислить количество $\Pi(x, L)$ простых чисел в интервале и сравнить с величиной $L/\ln(x)$. При каких условиях $\Pi(x, L)/L$ близко к $1/\ln(x)$ при заданных $x = 2000$, $L = 500$, количество простых чисел для деления 5-15, количество оснований 1-2?

Задание 5. Найти в интервале $(1000, 1000 + 300)$ все простые числа. Пусть $L(i)$ - разность между двумя соседними простыми числами. Построить гистограмму для $L(i)$. Вычислить выборочное среднее $L_{ср}$. Сравнить с величиной $\ln(x)$, где x - середина интервала. Задано: количество простых чисел для деления 5-20, количество оснований 1-3.

Задание 6. Для заданного набора чисел $\{k\}$ оценить относительную погрешность формулы для k -го простого числа:

$$p(k) = k/\ln(k), k = \{10, 15, 20, 30, 35\}.$$

Задание 7. В интервале $(500, 500 + 200)$ построить график относительного количества натуральных чисел, проходящих «решето Эратосфена», т.е. не делящихся на первые k простых. Расчет производится для всех $k \leq 10$.

в) Критерии оценивания компетенций (результатов)

Уровень сформированности компетенций оценивается по результатам ответов на вопросы и решения практической задачи.

Критерием оценивания ответов на теоретические вопросы к экзамену является полнота знаний теоретического материала в области математического и имитационного моделирования экономических процессов, умение излагать материал, отстаивать свою точку зрения, приводить практические примеры используемых в практике экономико-математических моделей.

Критерием оценивания результатов решения практического задания являются умения применять знания систем имитационного моделирования для решения практических задач.

г) Описание шкалы оценивания

Оценка осуществляется по 4-балльной шкале: отлично, хорошо, удовлетворительно, неудовлетворительно.

«Отлично» – выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания разделов учебной программы дисциплины (студент дал полные, развернутые ответы на все два вопроса в экзаменационном билете, ответил также на дополнительные вопросы преподавателя и безошибочно решил практическое задание).

«Хорошо» – выставляется студенту, показавшему полные знания разделов учебной программы дисциплины, но допустившему в ответе некоторые неточности (студент дал полные ответы на все два вопроса в экзаменационном билете, ответил также на дополнительные вопросы преподавателя и решил практическое задание. Но при ответе на вопросы, содержащиеся в билете, либо при выполнении практического задания им были допущены неточности).

«Удовлетворительно» – выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, но при этом он владеет основными разделами учебной программы (студент ответил на один вопрос билета и решил практическую задачу либо ответил на два вопроса билета, но не решил задачу).

«Неудовлетворительно» – выставляется студенту, ответ которого содержит существенные пробелы в знании содержания учебной программы дисциплины. Было сделано одно из заданий экзаменационного билета: студент решил задачу, но не ответил на теоретические вопросы или наоборот – ответил на один вопрос, но не решил задачу. Либо не было выполнено ни одного задания.

6.2.2 Оценочные средства текущего контроля

Оценочными средствами являются: устные доклады, отчеты по лабораторным работам, тест.

Устные доклады

а) Тематика устных докладов

1. Политика информационной безопасности предприятия.
2. Нормативно-правовая база обеспечения информационной безопасности предприятия.
3. Содержание основных законов Российской Федерации в сфере компьютерного права.
4. Законодательная база РФ по вопросам защиты информации.
5. Комплексный подход к обеспечению информационной безопасности.
6. Законодательные и нормативные акты РФ о предпринимательской деятельности.
7. Машинное представление информации.
8. Виды и формы представления информации.
9. Информация как объект права собственности.
10. Информация как коммерческая тайна.
11. Информация как рыночный продукт.
12. Элементы и объекты защиты в АС.
13. Основные виды вирусов и схемы их функционирования.
14. Обнаружение вирусов и меры по защите и профилактике
15. Основные меры защиты от вирусов.

16. Программно-технические меры обеспечения информационной безопасности.
17. Обеспечение информационной безопасности средствами Windows 7.
18. Безопасное хранение данных на основе шифрования.
19. Американский стандарт шифрования данных DES.
20. Стандарт шифрования данных ГОСТ 28147-89.
21. Система цифровой телефонии.
22. Системы шифрования с открытыми ключами.
23. Цифровые подписи на основе шифросистем с открытыми ключами.
24. Комплексный подход к обеспечению информационной безопасности:
25. Механические системы защиты
26. Оборонительные системы
27. Технические средства обеспечения безопасности подвижных объектов
28. Системы охранной сигнализации
29. Защита интеллектуальной собственности в РФ на современном этапе

б) критерии оценивания

Критериями оценивания доклада являются полнота раскрытия темы, степень ее проработанности, последовательность изложения материала; умения студента самостоятельно работать с литературой и информационно-электронными ресурсами, аргументированно и ясно строить речь, эффективно и наглядно представлять содержание результатов своей работы, а также владения навыками дискуссии и публичной защиты результатов своих исследований.

в) описание шкалы оценивания

Устные доклады оцениваются по шкале «зачтено» / «незачтено».

«Зачтено» выставляется в случае, если студент свободно излагает материал по заданному вопросу, опираясь при этом на литературные и другие дополнительные источники, отвечает на дополнительные уточняющие вопросы преподавателя и аудитории студентов, приводит практические примеры, аргументированно отстаивает свою точку зрения; во время доклада использует раздаточный материал и (или) презентацию.

«Незачтено» выставляется в случае, если в изложении наблюдаются значительные пробелы в знании материала и (или) студент не отвечает на дополнительные уточняющие вопросы и (или) не использует иллюстративный материал.

Отчет по лабораторным работам

а) разделы отчета

- наименование лабораторной работы;
- постановка задачи, исходные данные;
- описание методов и способов решения;
- этапы решения задачи и (или) ее алгоритмическое обеспечение;
- результаты, представленные в виде таблиц, графиков и т.п. с краткими пояснениями;
- выводы.

б) критерии оценивания

Студент должен продемонстрировать:

умения применять математические методы для формализации и решения прикладных задач; строить модели экономических процессов, исследовать их и

вырабатывать рекомендации к их применению на практике; организовывать вычислительный эксперимент на компьютере для исследования поведения экономических объектов, систем, процессов;

владение навыками работы с пакетами прикладных программ для моделирования и анализа экономических процессов.

в) описание шкалы оценивания

«Зачтено» выставляется в случае, если студент выполнил в полном объеме лабораторную работу, не допустил ошибок в расчетах, сделал выводы, свободно излагает этапы решения и результаты работы.

«Незачтено» выставляется в случае, если студент не выполнил лабораторную работу, либо выполнил, но допустил существенные ошибки в расчетах и (или) не сделал выводы, и (или) не может изложить этапы решения и результаты работы.

Тест

а) типовые задания к тесту

Формы тестовых заданий:

- выбор правильных ответов из перечисленных;
- установление правильной последовательности;
- установление соответствия.

б) критерии оценивания

Критерием оценивания теста является количество правильно выполненных тестовых заданий, свидетельствующих о полноте знаний теоретического материала в области экономико-математического моделирования.

в) описание шкалы оценивания

«Отлично» - процент правильно выполненных заданий составляет от 80% до 100.

«Хорошо» - процент правильно выполненных заданий составляет от 60% до 79.

«Удовлетворительно» - процент правильно выполненных заданий составляет от 50% до 59%.

«Неудовлетворительно» - процент правильно выполненных заданий составляет менее 50%.

6.3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

№ п/п	Наименование оценочного средства	Краткая характеристика процедуры оценивания компетенций	Представление оценочного средства в фонде
1.	Устные доклады	Доклады заслушиваются в начале практического занятия после изучения соответствующей темы. Продолжительность доклада не более 5 минут. Время на коллективное обсуждение 3-5 минут. В ходе заслушивания докладов проверяется способность студента самостоятельно приобретать новые знания, умения работать с информацией, литературными источниками, умения излагать результаты своих исследований, а также вести дискуссию, отстаивать свою точку зрения, приводя обоснованные аргументы, поддерживать интерес аудитории.	Перечень тем докладов, сгруппированных по темам лекционного курса.
2.	Отчет по лабораторным работам	Отчет готовится по каждой лабораторной работе. Отчеты принимаются индивидуально у каждого студента в течение лабораторного занятия. Проводится также собеседование, в ходе которого можно проверить знания терминологии, основных методов математического и имитационного моделирования, а также умения студента представлять результаты своей работы и аргументированно отстаивать свою точку зрения.	Комплект заданий к лабораторным работам
3.	Тест	Проводится на последнем аудиторном занятии. Тестирование проводится на бумажных носителях. Время на выполнение тестовых заданий составляет 1,5 часа. Результаты тестирования позволяют оценить уровень теоретической подготовленности студента.	Тестовые задания

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

а) Основная литература

1. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ: НИЦ ИНФРА—М, 2013. — 592 с. — Режим доступа: <http://www.znaniyum.com/bookread.php?book=402686>
2. Партыка Т. Л. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2008. - 432 с.: ил.; 60х90 1/16. - (Проф. обр.). (п) ISBN 978-5-91134-246-3 Режим доступа: <http://znaniyum.com/bookread.php?book=167284>

б) Дополнительная литература

1. Стратегия информационной безопасности и инновационной политики [Текст] / Под ред. Е. А. Олейникова. - М.: ВА им. Ф.Э. Дзержинского, 2003. - 271 с.
2. Экономическая безопасность: производство — финансы — банки/ Под ред. В. К. Сенчагова.- М.: ЗАО "Финстатинформ", 2000. - 621 с.
3. Ярочкин, В. И. Служба безопасности коммерческого предприятия [Текст] / В. И. Ярочкин. - М.: Ось-89, 1999. - 144 с.
4. Романец, Ю.В. Защита информации в компьютерных системах и сетях [Текст] / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. — 2-е изд., перераб. и доп. — М.: радио и связь, 2001 г. — 376 с.
5. Вопросы инновационной политики и экономической безопасности деятельности предприятий [Текст] / Под ред. Е. А. Олейникова. - М.: РЭА им. Г. В. Плеханова, 1992. - 210 с.
6. Гончаренко, Л. П. Экономическая и информационная модели создания системы безопасности личности [Текст] / Л. П. Гончаренко // Проблемы национальной безопасности. - М.: Ун-т дружбы народов, 1998. - С. 62—69.
7. Илларионов, А.С. Критерии экономической безопасности [Текст] / А.С. Илларионов // Вопросы экономики. - 1998. №10. - С. 35—58.
8. Матвеев, Н.В. Анализ методов исследования экономической безопасности [Текст]: Учеб.-метод. пособие для дистанционного обучения / Н.В. Матвеев. - М.: Рос.экон. акад., 1998. - 29 с.

8. Перечень ресурсов информационно-телекоммуникационной сети «интернет», необходимых для освоения дисциплины

- Электронная библиотека механико-математического факультета Московского государственного университета – www.lib.mexmat.ru/bookks/41
- Новая электронная библиотека – www.newlibrary.ru
- Российское образование (федеральный портал) – www.edu.ru
- Нехудожественная библиотека – www.nehudlit.ru
- Научная электронная библиотека www.e-library.ru
- Университетская информационная система www.uisrussia.ru

9. Методические указания для обучающихся по освоению дисциплины

Подготовка к лабораторным занятиям

При подготовке к лабораторным занятиям студент должен изучить теоретический материал по теме занятия (использовать конспект лекций, изучить основную литературу, ознакомиться с дополнительной литературой, при необходимости дополнить конспект, делая в нем соответствующие записи из литературных источников). В случае затруднений, возникающих при освоении теоретического материала, студенту следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения.

В начале лабораторного занятия преподаватель знакомит студентов с темой, оглашает план проведения занятия, выдает задание. В течение отведенного времени на выполнение работы студент может обратиться к преподавателю за консультацией или разъяснениями. В конце занятия проводится прием выполненных работ: проверка отчета, собеседование со студентом.

Результаты выполнения лабораторных работ оцениваются как текущая работа на «зачтено»/«незачтено».

Подготовка к устному докладу

Доклады делаются по каждой теме с целью проверки теоретических знаний студента, его способности самостоятельно приобретать новые знания, работать с информационными ресурсами и извлекать нужную информацию.

Доклады заслушиваются в начале лабораторного занятия после изучения соответствующей темы. Продолжительность доклада не должна превышать 5 минут. Тему доклада студент выбирает по желанию из предложенного списка.

При подготовке доклада студент должен изучить теоретический материал, используя основную и дополнительную литературу, обязательно составить план доклада (перечень рассматриваемых им вопросов, отражающих структуру и последовательность материала), подготовить раздаточный материал или презентацию. План доклада необходимо предварительно согласовать с преподавателем.

Выступление должно строиться свободно, убедительно и аргументировано. Преподаватель следит, чтобы выступление не сводилось к простому воспроизведению текста, не допускается простое чтение составленного конспекта доклада. Выступающий также должен быть готовым к вопросам аудитории и дискуссии.

Подготовка к тесту

При подготовке к тесту необходимо изучить темы 1-7. С целью оказания помощи студентам при подготовке к тесту преподавателем проводится групповая консультация с целью разъяснения наиболее сложных вопросов теоретического материала.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

№	Наименование раздела дисциплины	Информационные технологии
1	Введение в предмет. Угрозы информационной безопасности	MS Power Point, MS Word
2	Основные понятия теории информационной безопасности	MS Power Point, MS Word
3	Программно-технические методы защиты	MS Visio, Delphi, MS Visual Studio
4	Криптографические методы защиты	MS Visio, Delphi, MS Visual Studio
5	Организационно-правовые методы информационной безопасности	MS Power Point, MS Excel, MS Word
6	Роль стандартов в обеспечении информационной безопасности	MS Excel, MS Power Point
7	Технологии построения защищенных систем	MS Visio, Delphi, MS Visual Studio

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения лекционных занятий: классная доска, место преподавателя, компьютер, проектор, экран, посадочные места для обучающихся. Программное обеспечение - MS PowerPoint для демонстрации слайдов.

Для проведения лабораторных занятий: компьютерный класс, оборудованный компьютерами (по количеству обучающихся в группе), объединенными в локальную сеть и имеющими выход в Интернет. Учебное программное обеспечение: MS PowerPoint, MS Excel, MS Word, MS Visio, Delphi, MS Visual Studio.

12. Иные сведения и (или) материалы

12.1. Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине

В соответствии с ФГОС 3+ ВПО по направлению подготовки 09.03.01 Информатика и вычислительная техника, «реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся...». Проведение занятий в интерактивной форме предусмотрено в рамках данной дисциплины в объеме 12 часов для студентов очной формы обучения и 6 часов для очно-заочной формы обучения.

Тема	Вид занятия/содержание занятия	Часы		Технология
		для очной формы	для очно-заочной формы	
Тема 3. Программно-технические методы защиты	Лабораторная работа. Исследование защиты с применением пароля, а также исследование методов противодействия атакам на пароль	4	2	Анализ конкретной ситуации: обучающиеся должны проанализировать предложенную конфигурацию защиты, определить уязвимые места и разработать методику их ликвидации.
Тема 4. Криптографические методы защиты	Лабораторная работа. Методы современной криптографии на примере программирования одного из предложенных алгоритмов	4	2	Выполнение работы с использованием компьютерных технологий – MS Visual Studio, Delphi.
Тема 7. Технологии построения защищенных систем	Лабораторная работа. Составление документа «Политика безопасности»	4	2	Выполнение работы с использованием компьютерных технологий – MS Visual Studio, Delphi.
ИТОГО		12	6	

Составитель (и):

Зайцев В.Н., аспирант,
ведущий специалист отдела автоматизации расчета заработной платы, кадрового и производственного учета
ООО «Синерго Софт Системс»

(фамилия, инициалы и должность преподавателя (ей))