

Подписано электронной подписью:

Вержицкий Данил Григорьевич

Должность: Директор КГПИ ФГБОУ ВО «КемГУ»

Дата и время: 2024-04-24 00:00:00

471086fad29a3b30e244c728abc3661ab35c9d50210def0e75e03a5b6fdf6436

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ

Кузбасский гуманитарно-педагогический институт
федерального государственного бюджетного образовательного учреждения
высшего образования
«Кемеровский государственный университет»

Факультет информатики, математики и экономики

УТВЕРЖДАЮ

Декан А.В. Фомина
«09» февраля 2023 г.

Рабочая программа дисциплины

К.М.05.05 Информационная безопасность

Направление

09.03.01 Информатика и вычислительная техника

Направленность (профиль) подготовки

«Автоматизированные системы обработки информации и управления»

Программа бакалавриата

Квалификация выпускника

бакалавр

Форма обучения

Очная

год набора 2022

Новокузнецк 2023

Оглавление

1	Цель дисциплины.....	3
1.1	Формируемые компетенции	3
1.2	Индикаторы достижения компетенций.....	3
1.3	Знания, умения, навыки (ЗУВ) по дисциплине.....	4
2	Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации.	5
3	Учебно-тематический план и содержание дисциплины.....	6
3.1	Учебно-тематический план	6
3.2	Содержание занятий по видам учебной работы	7
4	Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации.	11
5	Материально-техническое, программное и учебно-методическое обеспечение дисциплины.....	12
5.1	Учебная литература	12
5.2	Материально-техническое и программное обеспечение дисциплины.	13
5.3	Современные профессиональные базы данных и информационные справочные системы.....	13
6	Иные сведения и (или) материалы.	13
6.1	Примерные темы письменных учебных работ	13
6.2	Примерные вопросы и задания / задачи для промежуточной аттестации.....	14

1 Цель дисциплины

В результате освоения данной дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы бакалавриата (далее ОПОП): ОПК-3.

Содержание компетенций как планируемых результатов обучения по дисциплине см. таблицы 1 и 2.

1.1 Формируемые компетенции

Таблица 1 - Формируемые дисциплиной компетенции

Наименование вида компетенции (универсальная, общепрофессиональная, профессиональная)	Код и название компетенции
Общепрофессиональная	ОПК-3Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

1.2 Индикаторы достижения компетенций

Таблица 2 – Индикаторы достижения компетенций, формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции по ОПОП	Дисциплины и практики, формирующие компетенцию ОПОП
ОПК-3Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	<p>ОПК-3.1. Формулирует профессиональные задачи в сфере проектирования, разработки, внедрения и эксплуатации средств вычислительной техники и информационных систем, управления их жизненным циклом, к решению которых в рамках освоения программы бакалавриата могут готовиться выпускники.</p> <p>ОПК-3.2. Осуществляет поиск источников информации по заданной теме своей профессиональной области в электронных информационных ресурсах по различным типам запросов.</p> <p>ОПК-3.3. Осуществляет информационно-библиографический поиск по заданной теме своей профессиональной области в печатных информационных ресурсах по различным типам запросов.</p> <p>ОПК-3.4. Осуществляет информационный поиск по заданной теме своей профессиональной области с применением информационно-</p>	<p>К.М.05 Современные информационные технологии и информационные системы</p> <p>К.М.05.02 Введение в профессиональную деятельность</p> <p>К.М.05.04 Операционные системы</p> <p>К.М.05.05 Информационная безопасность</p> <p>К.М.05.08 Сети и телекоммуникации</p> <p>К.М.05.14(У) Технологическая (проектно-технологическая) практика</p> <p>К.М.09 Государственная итоговая аттестация</p> <p>К.М.09.01(Д) Выполнение и защита выпускной квалификационной работы</p>

	<p>коммуникационных технологий в современных профессиональных базах данных и информационных справочных системах.</p> <p>ОПК-3.5. Выявляет угрозы информационной безопасности;</p> <p>ОПК-3.6. Анализирует и выбирает методы и средства обеспечения информационной безопасности в соответствии с заданием.</p> <p>ОПК-3.7. Эксплуатирует программно-аппаратные средства в сетевых структурах.</p>	
--	--	--

1.3 Знания, умения, навыки (ЗУВ) по дисциплине

Таблица 3 – Знания, умения, навыки, формируемые дисциплиной

Код компетенции	Формируемые компетенции	Дескрипторные характеристики компетенций
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационных коммуникационных технологий и с учетом основных требований информационной безопасности;	ОПК-3.5. Выявляет угрозы информационной безопасности; ОПК-3.6. Анализирует и выбирает методы и средства обеспечения информационной безопасности в соответствии с заданием.	<p>Знать:</p> <ul style="list-style-type: none"> – базовые понятия информационной безопасности; – классификацию угроз уязвимостей; – нормативно-правовую базу в области защиты информации; – основные понятия и методы организационно-правового, программно-аппаратного, криптографического обеспечения информационной безопасности; – методики построения систем защиты информации. <p>Уметь:</p> <ul style="list-style-type: none"> – моделировать угрозы и уязвимости информационной безопасности; – выделять источники информации, объекты защищаемой информации; – формировать требования к построению безопасной системы; – определять функциональные задачи и требования. <p>Владеть:</p> <ul style="list-style-type: none"> – методами организационно-правового, программно-аппаратного, криптографического обеспечения информационной безопасности; – методами и методиками построения систем защиты информации; – программными продуктами для оценки риска информационной безопасности; – программными средствами обеспечения информационной безопасности; – протоколами аутентификации, распределения ключей, электронной подписи и финансовой криптографии.

2 Объем и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации.

Таблица 4 – Объем и трудоёмкость дисциплины по видам учебных занятий

Общая трудоёмкость и виды учебной работы по дисциплине, проводимые в разных формах	Объём часов по формам обучения		
	ОФО	ОЗФО	ЗФО
1 Общая трудоёмкость дисциплины	180		
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	54		
Аудиторная работа (всего):	54		
в том числе:			
лекции	18		
практические занятия, семинары	36		
практикумы			
лабораторные работы			
в интерактивной форме			
в электронной форме			
Внеаудиторная работа (всего):			
в том числе, индивидуальная работа обучающихся с преподавателем			
подготовка курсовой работы/контактная работа			
групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем)			
творческая работа (эссе)			
3 Самостоятельная работа обучающихся (всего)	90		
4 Промежуточная аттестация обучающегося – экзамен – 5 семестр	36		

3 Учебно-тематический план и содержание дисциплины.

3.1 Учебно-тематический план

Таблица 5 - Учебно-тематический план очной формы обучения

№ п/п	Раздел дисциплины	Общая трудоемкость (часов)	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостояте льная работа обучающих ся	
			все го	лекци и семинары, практическ ие занятия		
1.	Введение в предмет. Угрозы информационной безопасности	16	2	6	7	Устный доклад; отчет по лабораторной работе.
2.	Основные понятия теории информационной безопасности	16	3	6	7	Устный доклад; Отчет по лабораторной работе.
3.	Программно- технические методы защиты	25	3	6	16	Устный доклад; Отчет по лабораторной работе.
4.	Криптографические методы защиты	25	3	6	16	Устный доклад; Отчет по лабораторной работе.
5.	Организационно правовые методы информационной безопасности	18	3	8	7	Устный доклад; Отчет по лабораторной работе.
6.	Роль стандартов в обеспечении информационной безопасности	18	3	8	7	Устный доклад; Отчет по лабораторной работе.
7.	Технологии построения защищенных систем	27	3	8	16	Устный доклад; Отчет по лабораторной работе
8.	Промежуточная аттестация -экзамен	36				
ИТОГО		180	18	36	90	

3.2 Содержание занятий по видам учебной работы

Таблица 6 – Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание
<i>Содержание лекционного курса</i>		
1	Введение в предмет. Угрозы информационной безопасности	<p>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.</p> <p>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.).</p> <p>Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности.</p> <p>Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.</p>
2	Основные понятия теории информационной безопасности	<p>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 монитора безопасности. Функции монитора безопасности.</p> <p>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.</p> <p>Анализ способов нарушений безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.</p>

№ п/п	Наименование раздела дисциплины	Содержание
3	Программно-технические методы защиты	<p>Общее представление о структуре защищенной информационной системы. Особенности современных информационных систем, факторы влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности.</p> <p>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.</p> <p>Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом.</p> <p>Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита.</p> <p>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.</p> <p>Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.</p>
4	Криптографические методы защиты	<p>Методы криптографии. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации.</p> <p>Причины нарушения безопасности информации при ее обработке СКЗИ (утечки информации по техническому каналу, неисправности в элементах СКЗИ, работа совместно с другими программами).</p> <p>Использование криптографических средств для решения задач идентификация и аутентификация.</p> <p>Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов информационной системы.</p> <p>Контроль за целостностью информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.</p>

№ п/п	Наименование раздела дисциплины	Содержание
5	Организационно правовые методы информационной безопасности	<p>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 безопасности.</p>
6	Роль стандартов в обеспечении информационной безопасности	<p>Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.</p> <p>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.</p> <p>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.</p> <p>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.</p>
7	Технологии построения защищенных систем	<p>Использование защищенных компьютерных систем. Общие принципы построения защищенных систем. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования.</p> <p>Исследование корректности реализации и</p>

№ п/п	Наименование раздела дисциплины	Содержание
		<p>верификации автоматизированных систем. Спецификация требований предъявляемых к системе.</p> <p>Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности</p>
<i>Содержание лабораторных занятий</i>		
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»

4 Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации.

Для положительной оценки по результатам освоения дисциплины обучающемуся необходимо выполнить все установленные виды учебной работы. Оценка результатов работы обучающегося в баллах (по видам) приведена в таблице 7.

Таблица 7 - Балльно-рейтинговая оценка результатов учебной работы обучающихся по видам (БРС)

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации	Баллы
Текущая учебная работа в семестре (Посещение занятий по расписанию и выполнение заданий)	80	Лекционные занятия (конспект) (10 занятий)	1 балл - посещение 1 лекционного занятия и выполнение задания на 51-85%	0-10
		Практические занятия (24 занятий).	24/50 балла - посещение 1 лекционного занятия и выполнение задания на 51-85% 24/520 балла - посещение 1 практического занятия и выполнение задания на 85.1-100%	0-50
Итого по текущей работе в семестре				0-60
Промежуточная аттестация (зачет с оценкой)	20	Теоретический вопрос 1	2 балла (пороговое значение) 10 баллов (максимальное значение)	2 - 10
		Теоретический вопрос 2	2 балла (пороговое значение) 10 баллов (максимальное значение)	2 - 10
Итого по промежуточной аттестации (зачет с оценкой)				4-20

5 Материально-техническое, программное и учебно-методическое обеспечение дисциплины.

5.1 Учебная литература

Основная учебная 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.znanium.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.; 60x90 1/16. - (Проф. обр.). (п) ISBN 978-5-91134-246-3
Режим доступа: <http://znanium.com/bookread.php?book=167284>

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.

5.2 Материально-техническое и программное обеспечение дисциплины.

Учебные занятия по дисциплине проводятся в учебных аудиториях КГПИ КемГУ:

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы	Перечень основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом
710 Учебная аудитория (мультимедийная) для проведения: - занятий лекционного типа.	Классная доска, место преподавателя, компьютер, проектор, экран, посадочные места для обучающихся. Программное обеспечение - MS PowerPoint для демонстрации слайдов.	654079, Кемеровская область, г. Новокузнецк, пр-кт Metallургов, д. 19
509 Компьютерный класс. Учебная аудитория (мультимедийная) для проведения: - занятий семинарского (практического) типа; - групповых и индивидуальных консультаций; - самостоятельной работы; - текущего контроля и промежуточной аттестации.	Компьютерный класс, оборудованный компьютерами (по количеству обучающихся в группе), объединенными в локальную сеть и имеющими выход в Интернет. Учебнопрограммное обеспечение: MS PowerPoint, MS Excel, MS Word, MS Visio, Delphi, MS Visual Studio.	654079, Кемеровская область, г. Новокузнецк, пр-кт Metallургов, д. 19

5.3 Современные профессиональные базы данных и информационные справочные системы.

- Электронная библиотека механико-математического факультета Московского государственного университета – www.lib.mexmat.ru/books/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.uirussia.ru

6 Иные сведения и (или) материалы.

6.1 Примерные темы письменных учебных работ

Письменные работы не предусмотрены.

6.2 Примерные вопросы и задания / задачи для промежуточной аттестации

Таблица 9 - Примерные теоретические вопросы и практические задания к экзамену

Разделы и темы	Примерные теоретические вопросы	Примерные практические задания и (или) задачи
1. Введение в предмет. Угрозы информационной безопасности.	<p>1. Что называется информационной безопасностью?</p> <p>2. Какие данные называются критическими?</p> <p>3. Какие вы знаете признаки компьютерных преступлений в интернет технологиях и какие основные технологии, и методы используются при совершении компьютерных преступлений?</p> <p>4. Какие четыре уровня защиты компьютерных (интернет технологий) и информационных ресурсов вы можете назвать?</p> <p>5. Перечислите признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности?</p>	<p><i>Задание 1.</i> Для одноалфавитного метода с задаваемым смещением выполнить шифрование с произвольным смещением.</p>
2. Основные понятия теории информационной безопасности.	<p>6. Перечислите меры защиты информационной безопасности?</p> <p>7. Какие меры предпринимают по защите целостности информации?</p> <p>8. Какие меры предпринимают по защите системных программ?</p> <p>9. Дублирование информации и его классы.</p> <p>10. Перечислите позиции административного уровня.</p> <p>11. Назовите цель ОНРВ и его основные положения?</p>	<p><i>Задание 2.</i> Для одноалфавитного метода с задаваемым смещением выполнить дешифрование зашифрованный шифром Цезаря текст.</p>
3. Программно-технические методы защиты.	<p>12. Что такое межсетевой экран и какая у него роль в защите.</p> <p>13. Законодательная</p>	<p><i>Задание 3.</i> Проверить на простоту два произвольных целых числа разрядностью 5.</p>

	<p>основа информационной безопасности, статьи и пр.</p> <p>14. Что такое политика безопасности на административном уровне?</p> <p>15. Основные принципы защиты информации на административном уровне?</p> <p>Средства Разграничения доступа.</p> <p>Что такое CGI процедуры, их назначения?</p> <p>Чем опасна программа, полученная из ненадежного источника, какие вы знаете средства контроля над такими программами?</p> <p>Как осуществляется защита WEB-серверов?</p>	
4. Криптографические методы защиты.	<p>20. Криптография и криптоанализ. Назначение криптографии.</p> <p>21. Перечислите известные алгоритмы шифрования. Цифровые деньги и их характеристики.</p> <p>22. Симметричная и асимметричная методология шифрования.</p> <p>23. Криптографические средства защиты.</p> <p>24. Квантовая криптография и ККС.</p>	<p><i>Задание 4.</i> 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?</p>
5. Организационно-правовые методы информационной безопасности.	<p>25. Чем определяется концепция обеспечения безопасности АСОИ.</p> <p>26. В чем состоит избирательная политика безопасности способом управления доступом.</p> <p>27. Организационные меры безопасности АСОИ.</p> <p>28. Матрица доступа в АСОИ.</p> <p>29. Полномочное управление доступом.</p> <p>30. Избирательное управление доступом.</p>	<p><i>Задание 5.</i> 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 $L_{\text{сред}}$. Сравнить с величиной $\ln(x)$, где x - середина интервала. Задано: количество простых чисел для деления 5-20, количество оснований 1-3.</p>
6. Роль стандартов в обеспечении	<p>31. Что такое универсальная</p>	<p><i>Задание 6.</i> Для заданного набора чисел $\{k\}$ оценить относительную</p>

информационной безопасности.	<p>операционная система?</p> <p>32. Что такое компьютерный вирус.</p> <p>33. Полиморфные вирусы.</p> <p>34. Суррогатные платежные средства.</p> <p>35. Файловые вирусы и алгоритм их работы.</p> <p>36. Особенность макровирусов.</p>	<p>погрешность формулы для k-го простого числа: $p(k) = k/\ln(k)$, $k = \{10, 15, 20, 30, 35\}$.</p>
7. Технологии построения защищенных систем.	<p>37. Полномочное управление доступом.</p> <p>38. Избирательное управление доступом.</p> <p>39. Отказоустойчивые компьютерные системы.</p> <p>40. Что вы понимаете под технологией RAID.</p> <p>41. Методы дублирования информации.</p>	<p><i>Задание 7.</i> 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 $k \leq 10$.</p>

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))