МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
«Информационные технологии»
_____ / Д.Г.Демидов /
«15» февраля 2024г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»

Направление подготовки
10.03.01 Информационная безопасность

Профиль
Безопасность компьютерных систем

Квалификация
Бакалавр

Формы обучения
Очная

Москва, 2024 г.

Разработчик(и):

Доцент кафедры «Информационная безопасность»,
Доцент. к.т.н.  /С.А. Кесель/

Согласовано:
Заведующий кафедрой «Информационная безопасность»  /И.В.Калуцкий/

Руководитель образовательной программы,  /А.Ю. Гневшев/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Основы информационной безопасности» следует отнести:

- раскрытие сущности и значения информационной безопасности и методов защиты информации в практических задачах и их место в системе национальной безопасности;
- формирование у студентов научного мировоззрения, понимания важности научно обоснованных методов для решения профессиональных задач в области безопасности информационных технологий.

К основным задачам освоения дисциплины «Основы информационной безопасности» следует отнести:

- овладение студентами понятийным аппаратом в области информационной безопасности и защиты информации; установление и раскрытие структуры угроз защищаемой информации;
- изучение базовых содержательных положений в области информационной безопасности и защиты информации; раскрытие современной доктрины информационной безопасности;
- раскрытие различных форм представления информации в проблемах обеспечения информационной безопасности;
- ознакомление с современными подходами к решению общей задачи – созданию комплексной(-ых) системы(-ем) защиты информации.

Обучение по дисциплине «Основы информационной безопасности» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.	ИОПК-1.1 Знает основные понятия информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных; ИОПК-1.2. Умеет использовать программные и аппаратные средства персонального компьютера; ИОПК-1.3. Владеет навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.).

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части (Б1.1), частью основной образовательной программы (Б1.1.8).

Дисциплина является базовой по своим компетенциям.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часов)

3.1 Виды учебной работы и трудоемкость

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры
1	**Аудиторные занятия**	**64**	**1**
	В том числе:		
1.1	Лекции	32	1
1.2	Семинарские/практические занятия		
1.3	Лабораторные занятия	32	1
2	**Самостоятельная работа**	**80**	**1**
3	**Промежуточная аттестация**		
	Экзамен		1
	Итого:	**144**	

3.2 Тематический план изучения дисциплины

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1. Защита информации как объективная закономерность эволюции постиндустриального общества.	**18**	4	-	4	-	10
2	Раздел 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты.	**18**	4	-	4	-	10
3	Раздел 3. Угрозы информационной безопасности в компьютерных системах.	**18**	4	-	4	-	10
4	Раздел 4. Общая характеристика средств и методов защиты информации	**18**	4	-	4	-	10
5	Раздел 5. Организационно-правовое обеспечение защиты информации.	**18**	4	-	4	-	10
6	Раздел 6. Защита компьютерных систем от несанкционированного вмешательства.	**18**	4	-	4	-	10

7	Раздел 7. Криптографические методы защиты информации.	**18**	4	-	4	-	10
8	Раздел 8. Комплексная защита информации в компьютерных системах.	**18**	4	-	4	-	10
Итого		**144**	**32**		**32**		**80**

3.3 Содержание дисциплины

Раздел 1. Защита информации как объективная закономерность эволюции постиндустриального общества.

Предмет, содержание и задачи курса, его место среди других дисциплин учебного плана. Формы отчетности, основная и дополнительная литература. Информация и ее роль в современном обществе. Эволюция информационных процессов и информационных отношений. Сущность и цели информатизации. Глобализация информационных отношений. Информационные технологии. Информационные ресурсы услуги. Объективная необходимость и общественная потребность в защите информации. Сущность защиты информации. Правовое регулирование вопросов защиты информации.

Раздел 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты.

Право на информацию в системе гражданских прав личности. Возможные ограничения. Массовая информация и информация ограниченного доступа. Неприкосновенность частной жизни, персональные данные. Виды тайн. Коммерческая тайна. Государственная тайна. Документированная информация как объект права собственности. Информационная безопасность как составляющая национальной безопасности РФ. Информационные войны, информационное оружие. Доктрина информационной безопасности РФ.

Раздел 3. Угрозы информационной безопасности в компьютерных системах.

Компьютерная система (КС) как объект защиты информации. Понятие угрозы информационной безопасности в КС. Классификация и общий анализ угроз информационной безопасности в КС. Случайные угрозы информационной безопасности. Преднамеренные угрозы информационной безопасности. Сбои и отказы. Общие сведения о кодах для обнаружения и исправления случайных ошибок. Система охраны объектов КС. Основные виды технических каналов утечки информации. Техника промышленного шпионажа. Общие сведения о компьютерных вирусах. Классификация компьютерных вирусов. Механизмы заражения компьютерными вирусами.

Раздел 4. Общая характеристика средств и методов защиты информации.

Эволюция концепции информационной безопасности в компьютерных системах. Реализация угроз информационной безопасности путём несанкционированного доступа. Модель поведения потенциального нарушителя Обобщённые модели систем защиты информации. Основные принципы обеспечения информационной безопасности в КС. Понятие комплексной системы защиты информации (КСЗИ).

Раздел 5. Организационно-правовое обеспечение защиты информации.

Общая характеристика организационного обеспечения защиты информации. Основные задачи службы безопасности предприятия. Организационные мероприятия, обеспечивающие защиту информации. Необходимость правового регулирования в области защиты информации. Законодательство РФ в этой области. Стандартизация в области обеспечения информационной безопасности; международные и отечественные нормативные и руководящие документы.

Раздел 6. Защита компьютерных систем от несанкционированного вмешательства.

Модели управления доступом к информации в КС. Идентификация и аутентификация пользователей и разграничение их доступа к компьютерным ресурсам. Защита программных средств от несанкционированного копирования и исследования. Защита от несанкционированного изменения структуры КС в процессе эксплуатации. Контроль целостности программ и данных в процессе эксплуатации. Регистрация и контроль действий пользователей.

Раздел 7. Криптографические методы защиты информации.

Основные понятия и этапы развития криптографии. Классификация криптографических средств. Основные методы шифрования. Шифрование методами замены и перестановки. Аналитические и аддитивные методы шифрования. Системы шифрования с открытым ключом.

Раздел 8. Концепция создания КСЗИ в КС. Технология разработки КСЗИ. Функционирование комплексных систем защиты информации. Аудит в защищенных КС. Организационная структура КСЗИ.

3.4 Тематика семинарских/практических занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные работы

Раздел 1. Защита информации как объективная закономерность эволюции постиндустриального общества.

Лабораторная работа №1.1. Роль информации в современном мире.

Лабораторная работа №1.2. Основные понятия в информационной безопасности.

Раздел 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты.

Лабораторная работа №2.1. Виды информации.

Лабораторная работа №2.2. Доктрина информационной безопасности РФ.

Раздел 3. Угрозы информационной безопасности в компьютерных системах.

Лабораторная работа №3.1. Классификация и общий анализ угроз информационной безопасности в КС.

Лабораторная работа №3.2. Система охраны объектов КС.

Раздел 4. Общая характеристика средств и методов защиты информации.

Лабораторная работа №4.1. Средства защиты информации в КС.

Лабораторная работа №4.2. Методы защиты информации в КС.

Раздел 5. Организационно-правовое обеспечение защиты информации.
Лабораторная работа №5.1. Основные задачи службы безопасности предприятия.
Лабораторная работа №5.2. Стандартизация в области обеспечения информационной безопасности.

Раздел 6. Защита компьютерных систем от несанкционированного вмешательства.
Лабораторная работа №6.1. Модели управления доступом к информации в КС.
Лабораторная работа №6.2. Регистрация и контроль действий пользователей.

Раздел 7. Криптографические методы защиты информации.
Лабораторная работа №7.1. Классификация криптографических средств.
Лабораторная работа №7.2. Аналитические и аддитивные методы шифрования.

Раздел 8. Комплексная защита информации в компьютерных системах.
Лабораторная работа №8.1. Технология разработки КСЗИ.
Лабораторная работа №8.2. Организационная структура КСЗИ.

3.5 Тематика курсовых проектов (курсовых работ)

Курсовое проектирование по дисциплине «Основы информационной безопасности» не предусмотрено учебным планом.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», текст: электронный, – URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264, режим доступа: свободный.

2. Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных», текст: электронный, – URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108261, режим доступа: свободный.

3. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Национальный стандарт РФ: введен 01.02.2008: - М.: Стандартинформ, 2008. – URL: https://protect.gost.ru/document.aspx?control=7&id=129024, режим доступа: свободный.

4.2 Основная литература

1. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449350.

2. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456793.

3. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. —

(Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456792.

4.3 Дополнительная литература

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772.

2. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449285.

3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451933.

4.4 Электронные образовательные ресурсы

ЭОР Разрабатывается.

4.5 Лицензионное и свободно распространяемое программное обеспечение

В рамках освоения дисциплины, дополнительное программное обеспечение не предусмотрено.

4.6 Современные профессиональные базы данных и информационные справочные материалы

В рамках освоения дисциплины, использование профессиональных баз данных и информационных справочных материалов не предусмотрено.

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого, допускается использование студентом собственной вычислительной техники (ноутбук).

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно телекоммуникационной сети «Интернет». Созданная информационно-

образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий. В процессе самостоятельной работы студентов предусмотрена возможность получения индивидуальных консультаций преподавателя с использованием электронной почты в сети Интернет.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

3. При организации и проведения экзаменов в практико-ориентированной форме следует использовать утвержденные кафедрой Методические рекомендации.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки **10.03.01 «Информационная безопасность».**

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции и лабораторные занятия.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Самостоятельная работа включает изучение теоретических и практических разделов дисциплины.

Общие рекомендации по организации самостоятельной работы:

Время, которым располагает студент для выполнения учебного плана, складывается из двух составляющих: одна из них – это аудиторная работа в вузе по расписанию занятий, другая –внеаудиторная самостоятельная работа. Задания и материалы для самостоятельной работы выдаются во время учебных занятий по расписанию, на этих же занятиях преподаватель осуществляет контроль за самостоятельной работой, а также оказывает помощь студентам по правильной организации работы.

Чтобы выполнить весь объем самостоятельной работы, необходимо заниматься по 1 – 4 часа ежедневно. Начинать самостоятельные внеаудиторные занятия следует с первых же дней семестра. Первые дни семестра очень важны для того, чтобы включиться в работу, установить определенный порядок, равномерный ритм на весь семестр. Ритм в работе –это ежедневные самостоятельные занятия, желательно в одни и те же часы, при целесообразном чередовании занятий с перерывами для отдыха.

Начиная работу, не нужно стремиться делать вначале самую тяжелую ее часть, надо выбрать что-нибудь среднее по трудности, затем перейти к более трудной работе. И

напоследок оставить легкую часть, требующую не столько больших интеллектуальных усилий, сколько определенных моторных действий (черчение, построение графиков и т.п.).

Следует правильно организовать свои занятия по времени: 50 минут –работа, 5-10 минут –перерыв; после 3 часов работы перерыв –20-25 минут. Иначе нарастающее утомление повлечет неустойчивость внимания. Очень существенным фактором, влияющим на повышение умственной работоспособности, являются систематические занятия физической культурой. Организация активного отдыха предусматривает чередование умственной и физической деятельности, что полностью восстанавливает работоспособность.

Методические указания к отдельным видам деятельности:

Лекция: Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, формулировки, выводы. Помечать важные мысли. Выделять ключевые слова, термины. Делать пометки на вопросах, терминах, блоках в тексте, которые вызвали затруднения, после чего постараться найти ответ в рекомендуемой литературе. Если ответ не найден, то на консультации обратиться к преподавателю.

Лабораторная работа: Работа с конспектом лекций и методическими указаниями по выполнению лабораторной работы, просмотр рекомендуемой литературы, конспектирование основных мыслей и выводов, разработка плана выполнения лабораторной работы, предварительная формулировка возможных выводов по работе. Подготовка к практическим занятиям, проработка материала по вопросам, выносимым на практические занятия. Для более углублённого изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темой.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: основные понятия информатики, назначение, функции и структуру операционных	Обучающийся не знает или в недостаточной степени знает основные понятия информатики,	Обучающийся демонстрирует частичное знание основных понятий информатики, назначения,	Обучающийся демонстрирует полное знание основных понятий информатики, назначения,	Обучающийся демонстрирует полное знание основных понятий информатики, назначения,

систем, вычислительных сетей и систем управления базами данных.	назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных.	функций и структуры операционных систем, вычислительных сетей и систем управления базами данных. . Допускаются значительные ошибки	функций и структуры операционных систем, вычислительных сетей и систем управления базами данных. . Допускаются незначительные ошибки, неточности	функций и структуры операционных систем, вычислительных сетей и систем управления базами данных. . Допускаются незначительные неточности
уметь: использовать программные и аппаратные средства персонального компьютера.	Обучающийся не умеет или в недостаточной степени умеет использовать программные и аппаратные средства персонального компьютера.	Обучающийся демонстрирует частичное умение использовать программные и аппаратные средства персонального компьютера. . Допускаются значительные ошибки	Обучающийся демонстрирует полное умение использовать программные и аппаратные средства персонального компьютера. . Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует полное умение использовать программные и аппаратные средства персонального компьютера. . Допускаются незначительные неточности
владеть: навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.).	Обучающийся не владеет или в недостаточной степени владеет навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационны	Обучающийся демонстрирует частичное владение навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов,	Обучающийся демонстрирует полное владение навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационны	Обучающийся демонстрирует полное владение навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки

	х материалов, СУБД и т.п.).	СУБД и т.п.). . Допускаются значительные ошибки	х материалов, СУБД и т.п.). . Допускаются незначительные ошибки, неточности	презентационн ых материалов, СУБД и т.п.). . Допускаются незначительны е неточности

Форма промежуточной аттестации: экзамен.

По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Текущий контроль

Текущий контроль успеваемости студентов осуществляется в процессе проведения лабораторных работ.

7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации

Экзамен

Список вопросов для экзамена

1. Информация как средство отражения окружающего мира и как средство его познания. Количественные оценки и показатели качества информации.
2. Эволюция информационных процессов в обществе. Информатизация и компьютеризация. Информационные ресурсы, продукты и услуги. Объективная необходимость и общественная потребность защиты информации.
3. Информационная безопасность личности, общества и государства. Массовая и конфиденциальная информация. Виды тайн.
4. Информационная безопасность как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.
5. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в КС. Классификация угроз.
6. Общая характеристика случайных угроз информационной безопасности в КС.
7. Общая характеристика преднамеренных угроз информационной безопасности в КС.
8. Эволюция концепции информационной безопасности в КС. Основные принципы обеспечения информационной безопасности в КС. Политика безопасности.
9. Реализация угроз информационной безопасности в КС путем несанкционированного доступа (НСД). Классификация каналов НСД. Собирательный образ потенциального нарушителя.
10. Обобщенные модели системы защиты информации в КС. Одноуровневые, многоуровневые и многозвенные модели. Общая характеристика средств и методов защиты информации в КС.
11. Общая характеристика организационных мероприятий, обеспечивающих информационную безопасность КС. Основные задачи службы безопасности.
12. Необходимость правового регулирования в области защиты информации. Информация как объект права собственности. Правоотношения собственника, и правообладателя информационных ресурсов.
13. Отечественное законодательство в области информации и защиты информации.
14. Ответственность за правонарушения при работе с компьютерными системами.
15. Эксплуатационная надежность КС как источник возникновения случайных угроз информационной безопасности. Пути ее повышения. Резервирование технических средств. Программно-аппаратный контроль и тестирование.
16. Оптимизация взаимодействия пользователя с КС как средство предотвращения ошибочных операций случайного характера.
17. Помехоустойчивое кодирование. Избыточные коды для обнаружения и исправления случайных ошибок в работе КС.

18. Дублирование информации как средство парирования угроз безопасности в КС. Многоуровневое дублирование. Технология RAID.
19. Минимизация ущерба, наносимого КС авариями и стихийными бедствиями.
20. Система охраны объектов КС.
21. Общая характеристика технических каналов утечки информации в КС.
22. Методы и средства защиты информации в КС от утечки по каналам побочных электромагнитных излучений и наводок.
23. Средства противодействия подслушивания и дистанционному наблюдению.
24. Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.
25. Идентификация и аутентификация субъектов доступа к ресурсам КС. Парольные методы и оценка их эффективности. Биометрические методы.
26. Средства и методы разграничения доступа к ресурсам КС.
27. Защита программных средств КС от несанкционированного копирования и исследования.
28. Защита от несанкционированного изменения структуры КС в процессе эксплуатации.
29. Общие понятия, история развития и классификация криптографических средств.
30. Общая характеристика различных методов шифрования. Криптостойкость. Шифрование с симметричным и несимметричным ключами.
31. Шифрование методом замены. Простая, полиалфавитная и многозначная замена.
32. Аналитические методы шифрования.
33. Шифрование методом гаммирования.
34. Отечественные и зарубежные стандарты шифрования.
35. Общая характеристика и классификация компьютерных вирусов.
36. Механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.
37. Средства, используемые для обнаружения компьютерных вирусов.
38. Профилактика заражения компьютерными вирусами.
39. Антивирусные средства для лечения и удаления компьютерных вирусов. Программыполифаги. Эвристические анализаторы.
40. Чем вызвана необходимость разработки стандартов по защите информации? Охарактеризуйте отечественные нормативы и зарубежные стандарты в этой области.
41. Содержательный смысл понятия комплексной системы защиты информации (КСЗИ) в компьютерных системах. Основные принципы и положения, реализующие системный подход к построению КСЗИ.
42. Функции и задачи защиты, механизмы защиты, уровень защищенности, управление защитой и другие базовые понятия, используемые при формировании КСЗИ.
43. Общетеоретическая постановка задачи оптимизации КСЗИ на основе выбранного критерия эффективности защиты.
44. Основные технологические этапы разработки КСЗИ.
45. Средства моделирования, применяемые для оптимизации КСЗИ.
46. Организационно-технические мероприятия, проводимые в процессе эксплуатации КСЗИ.
47. Задачи, решаемые подсистемой аудита в составе защищенных КС.

Пример билета.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1
по дисциплине

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки
10.03.01 Информационная безопасность

ВОПРОСЫ:

1. Общая характеристика преднамеренных угроз информационной безопасности в КС.
2. Оптимизация взаимодействия пользователя с КС как средство предотвращения ошибочных операций случайного характера.
3. Защита от несанкционированного изменения структуры КС в процессе эксплуатации.

Утверждено: _____ / _____ / «__» _____ 20__г.