Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 05.09.2026 12:33:11
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»

Направление подготовки
«10.05.03 Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист

Формы обучения
Очная

Москва, 2026 г.

Разработчик(и):

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

Ассистент кафедры «Информационная безопасность»  /А.В. Шорников/

Согласовано:
Заведующий кафедрой «Информационная безопасность»,
к.т.н., доцент  /И.В. Калуцкий/

Руководитель образовательной программы
ст. преподаватель кафедры «Информационная безопасность»  /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 «Дисциплины (модули)».

Дисциплина является базовой по своим компетенциям, обеспечивает изучение дисциплин: «Аналитика информационной безопасности», «Аудит информационной безопасности», «Организационно-правовое обеспечение информационной безопасности» и подготовку выпускной квалификационной работы.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).

3.1 Виды учебной работы и трудоемкость
(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**64**	**1**	3-18
	В том числе:			
1.1	Лекции	32	1	3-18
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	32	1	3-18
2	**Самостоятельная работа**	**80**	**1**	3-18
3	**Промежуточная аттестация**		**1**	19-21
	Экзамен		1	19-21
	Итого	**144**		

3.1.2 Очно-заочная форма обучения

Не предусмотрена.

3.1.3 Заочная форма обучения

Не предусмотрена.

3.2 Тематический план изучения дисциплины

(по формам обучения)

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**

3.2.2 Очно-заочная форма обучения

Не предусмотрена

3.2.3 Заочная форма обучения

Не предусмотрена

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 и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные занятия

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)

Не предусмотрены учебным планом.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 года № 149-ФЗ: [в актуальной редакции]. Доступ из справочно-правовой системы «КонсультантПлюс». – Текст: электронный.
2. О персональных данных: Федеральный закон от 27 июля 2006 года № 152-ФЗ: [в актуальной редакции]. Доступ из справочно-правовой системы «КонсультантПлюс». – Текст: электронный.
3. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 12 июля 2017 года № 187-ФЗ: [в актуальной редакции]. Доступ из справочно-правовой системы «КонсультантПлюс». – Текст: электронный.
4. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 05 декабря 2016 года № 646 // Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7076.
5. О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 02 июля 2021 года № 400 // Собрание законодательства Российской Федерации. – 2021. – № 27 (часть II). – Ст. 5351.
6. Об утверждении перечня сведений конфиденциального характера: указ Президента Российской Федерации от 06 марта 1997 года № 188 // Собрание законодательства Российской Федерации. – 1997. – № 10. – Ст. 1127.
7. Об утверждении перечня сведений, отнесенных к государственной тайне: указ Президента Российской Федерации от 30 ноября 1995 года № 1203 // Собрание законодательства Российской Федерации. – 1995. – № 49. – Ст. 4775.
8. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Москва: Стандартинформ, 2006. – 12 с.
9. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – Москва: Стандартинформ, 2006. – 16 с.
10. ГОСТ Р 7.32-2017. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления. – Москва: Стандартинформ, 2017. – 28 с.

4.2 Основная литература

1. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие для вузов / Е. К. Баранова, А. В. Бабаш. – 4-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2024. – 322 с. – (Высшее образование). – ISBN 978-5-534-15488-8.
2. Малюк, А. А. Введение в информационную безопасность: учебное пособие для студентов вузов / А. А. Малюк. – 2-е изд. – Москва: Горячая линия - Телеком, 2022. – 288 с. – ISBN 978-5-9912-0941-0.
3. Гришина, Н. В. Организация комплексной системы защиты информации: учебник для вузов / Н. В. Гришина. – Москва: Гелиос АРВ, 2021. – 304 с. – ISBN 978-5-85438-293-9.

4.3 Дополнительная литература

1. Бабаш, А. В. Криптографические методы защиты информации: учебник и практикум для вузов / А. В. Бабаш, Е. К. Баранова. – Москва: Издательство Юрайт, 2024. – 190 с. – (Высшее образование). – ISBN 978-5-534-15990-6.
2. Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. – 2-е изд., перераб. и доп. – Санкт-Петербург: БХВ-Петербург, 2023. – 432 с. – ISBN 978-5-9775-1178-0.
3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. – Москва: ИД «ФОРУМ»: ИНФРА-М, 2022. – 416 с. – ISBN 978-5-16-015335-3.

4.4 Электронные образовательные ресурсы

Электронный курс «Основы информационной безопасности» [Электронный ресурс] // Электронная информационно-образовательная среда Московского политеха / URL: https://online.mospolytech.ru/course/view.php?id=561.

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 системы

1. КонсультантПлюс: справочная правовая система [Электронный ресурс]. – Режим доступа: свободный. URL: https://www.consultant.ru/.
2. Гарант: информационно-правовой портал [Электронный ресурс]. – Режим доступа: свободный. URL: https://www.garant.ru/
3. eLIBRARY.RU: научная электронная библиотека [Электронный ресурс]. – Режим доступа: свободный. URL: https://elibrary.ru/.
4. Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/ – Режим доступа: для авториз. пользователей.
5. Образовательная платформа «Юрайт» : [сайт]. – URL: https://urait.ru/ – Режим доступа: для авториз. пользователей.
6. Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprsmart.ru/ – Режим доступа: для авториз. пользователей.

5 Материально-техническое обеспечение

Лабораторные работы и самостоятельная работа студентов должны проводиться в специализированной аудитории, оснащенной современной оргтехникой и персональными компьютерами с программным обеспечением в соответствии с тематикой изучаемого материала. Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов. Рабочее место преподавателя должно быть оснащено современным компьютером с подключенным к нему проектором на настенный экран, или иным аналогичным по функциональному назначению оборудованием.

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.

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 является самостоятельная работа, а также посещение аудиторных занятий.

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

На занятиях студентов, в том числе предполагающих практическую деятельность, осуществляется закрепление полученных, в том числе и в процессе самостоятельной работы, знаний. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста.

Самостоятельная работа осуществляется индивидуально. Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на аудиторных занятиях. Оценивание результатов обучения по дисциплине осуществляется на основе балльно-рейтинговой системы (далее – БРС). Максимальный совокупный балл за академический период составляет 100.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

Приветствуется обсуждение самих заданий с другими студентами: можно как давать, так и получать советы по общей стратегии выполнения и изучения материала, давать и получать помощь в проверке гипотез и задумок. Однако выполнять задания и оформлять отчетные материалы студент должен самостоятельно. Делиться отчетными материалами или создавать их совместно запрещено.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

Приведенные ниже правила выставления оценок могут быть изменены, если преподаватель сочтет это необходимым. Важно, чтобы обучающиеся регулярно просматривали план курса, выложенный в СДО, на предмет его обновления или изменения. Достижение компетенций оценивается с помощью лабораторных работ и рубежных контролей. По усмотрению преподавателя студенту могут начисляться дополнительные баллы за активную работу в семестре, участие в научных мероприятиях, нестандартные решения задач и другие достижения. Такие баллы суммируются с основной оценкой, но итоговый результат не может превышать 100 баллов.

После сдачи (загрузки в СДО) лабораторной работы студент должен ее защитить. Во время защиты лабораторной работы преподаватель проверяет содержание отчета, таблиц, исходного кода и других отчетных материалов, а также выполнение критериев и требований задания, а студент отвечает на вопросы преподавателя по предоставленным отчетным материалам, а также теоретическим вопросам, приведенных после текста задания лабораторной работы (при их наличии). Если студент отказывается отвечать на вопросы, или дает полностью неверные ответы, или ответы не по теме, то работа может считаться сданной, но при этом она не оценивается, либо оценка будет снижена на усмотрение преподавателя.

За каждую лабораторную работу устанавливается максимально возможное количество рейтинговых баллов в соответствии с пунктом 7.2. При несвоевременной сдаче работы (позднее срока, установленного в календарно-тематическом плане) количество начисляемых баллов может быть снижено:

- при сдаче работы с опозданием до 3 календарных дней – максимально возможное количество баллов снижается на 10% (оценка за лабораторную работу выставляется с коэффициентом – 0.9);
- при сдаче работы с опозданием от 4 до 7 календарных дней – максимально возможное количество баллов снижается на 25% (оценка за лабораторную работу выставляется с коэффициентом – 0.75);
- при сдаче работы с опозданием свыше 7 календарных дней – начисляется не более 50% от максимально возможного количества баллов за задание (оценка за лабораторную работу выставляется с коэффициентом – 0.5).

В случае наличия уважительных причин для несвоевременной сдачи работы, студент должен обратиться к преподавателю. При возможности, студенты должны заранее сообщать о том, что у них могут возникнуть трудности со своевременной сдачей лабораторной работы или иного полученного задания.

Работа должна быть выполнена студентом самостоятельно: в отчетных материалах должны содержаться результаты работы только за его авторством, по отчетным материалам можно проследить как велась работа, студент может объяснить ход выполнения работы, если же обозначенное выше не соблюдается, то такая работа не считается сданной и не оценивается.

Рубежные контроли выполняются в аудитории индивидуально по варианту задания, выданному преподавателем в назначенные дни. При отсутствии студента в день написания

контрольной работы ему дается еще один шанс ее написать на другом занятии в семестре (в том числе и в рамках консультаций преподавателя), но обязательно очно.

7.2 Шкала и критерии оценивания результатов обучения

За посещение аудиторных занятий начисляется до 9 баллов (по 0,5 балла за каждое занятие при условии регулярного посещения). При пропуске занятий количество баллов уменьшается пропорционально количеству пропусков.

За выполнение лабораторных работ начисляется до 47 баллов, более конкретное распределение баллов за лабораторные работы представлено ниже:

Лабораторные работы №1.1, №1.2, №2.1, №2.2, №4.2, №5.1 – до 2 баллов.

Лабораторные работы №3.1, №4.1, №5.2, №7.1, №8.1 – до 3 баллов.

Лабораторные работы №3.2, №6.1, №6.2, №7.2, №8.2 – до 4 баллов.

За прохождение рубежного контроля начисляется до 8 баллов. За первый и второй рубежный контроль можно получить до 2 баллов, за третий рубежный контроль можно получить до 3 баллов.

Итого, по результатам текущего контроля, не считая дополнительных баллов, студент может получить до 64 баллов.

В свою очередь, по результатам промежуточной аттестации студент может получить до 36 баллов. Студенты, получившие оценку «неудовлетворительно» в ходе промежуточной аттестации, сохраняют ранее накопленную оценку за текущий контроль.

Итоговая оценка по дисциплине (модулю) определяется по следующим критериям:

- «неудовлетворительно» (2) – 0-54 баллов;
- «удовлетворительно» (3) – 55-69 баллов;
- «хорошо» (4) – 70-84 баллов;
- «отлично» (5) – 85-100 баллов.

7.3 Оценочные средства

7.3.1 Текущий контроль

Оценочными средствами текущего контроля являются лабораторные работы, выложенные в курсе СДО по данной дисциплине (модулю), а также прохождение рубежных контролей.

7.3.2 Промежуточная аттестация

Формой оценки знаний в рамках промежуточной аттестации является: ***экзамен***.

В ходе промежуточной аттестации студенту выдается билет, содержащий 3 вопроса. За ответ на каждый вопрос студент может получить до 12 баллов. Билет формируется из перечня вопросов, расположенного ниже:

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 экзаменационного билета

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

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №_
по дисциплине

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

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.