МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ФГОУ ВПО «Уральский государственный лесотехнический университет»

Кафедра Социально-культурных технологий

Одобрена:
Кафедрой СКТ
Протокол от 19.09. 2012г.
Зав. каф. _____

Утверждаю
Декан гуманитарного факультета
Светлова И.Г. _____
«29» 09 2012г.

Методическая комиссия
гуманитарного факультета
Протокол от 28.09. 2012г.
Председатель _____ Бородина Е.В.

ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б.2.ДВ.2. Информационная безопасность в СКС

Направление: 100100.62 «Сервис»
Профиль
Квалификация бакалавр
Трудоемкость: 108 ч (3 зачетные единицы)

Разработчик учебной программы _____ доцент каф. СКТ Байчибаева А.В.

Екатеринбург 2012г.

Введение

Дисциплина направлена на формирование у студентов системных знаний по проблеме обеспечения комплексной защиты информационных ресурсов и управлению информационными рисками, а также практических навыков безопасной работы в информационных системах.

Изучение дисциплины позволит студентам овладеть основами методологии оценки информационных рисков, выбора механизмов защиты информационных ресурсов, построения интегрированной системы обеспечения информационной безопасности предприятия, ведения защищенного электронного бизнеса и электронного банкинга.

В процессе обучения существенное место отводится подготовке к практической работе в защищенных информационных системах. Студенты осваивают методы анализа реальных угроз безопасности информационным ресурсам, приобретают навыки использования встроенных возможностей операционной системы, приложений MS Office, брандмауэра, Internet Explorer, антивирусных и криптографических средств, а также знакомятся с приемами работы в системе защищенного документооборота, электронного бизнеса и банкинга.

2. Цели и задачи дисциплины

Цели изучения дисциплины

Целью изучения дисциплины является ознакомление студентов с:

- основными понятиями и определениями информационной безопасности;
- источниками, рисками и формами атак на информацию;
- угрозами, которыми подвергается информация;
- вредоносными программами.
- защитой от компьютерных вирусов и других вредоносных программам;

- методами и средствами защиты информации;
- политикой безопасности компании в области информационной безопасности;
- стандартами информационной безопасности;
- криптографическими методами и алгоритмами шифрования информации;
- алгоритмами аутентификации пользователей;
- защитой информации в сетях;
- требованиям к системам защиты информации.

Задачи изучения дисциплины

Задача курса: ознакомить студентов с тенденциями развития защиты информационной с моделями возможных угроз, терминологией и основными понятиями теории защиты информации, а так же с нормативными документами и методами защиты компьютерной информации.

3. Требования к знания умениям и навыкам

Компетентностная модель выпускника

Выпускник вуза по направлению 100100 в соответствии с ГОС ВПО третьего поколения должен обладать следующими компетенциями:
Общекультурными:

- использовать базовые положения математики, естественных, гуманитарных и экономических наук при решении социальных и профессиональных задач (ОК-2);

- понимать сущность и значение информации в развитии современного информационного общества, соблюдать основные требования информационной безопасности (ОК-12);

- владеть основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления информацией; работать с информацией в глобальных компьютерных сетях (ОК-13);

- участвовать в работе над инновационными проектами, используя базовые методы исследовательской деятельности (ОК-14);

Профессиональными компетенциями (ПК):
производственно-технологическая деятельность:

- готовностью внедрять и использовать современные информационные технологии в процессе профессиональной деятельности (ПК-7);

организационно-управленческая деятельность:

- к организации технологического процесса сервиса (ПК-12);
- готовностью к изучению научно-технической информации, отечественного и зарубежного опыта в сервисной деятельности (ПК-13);

До начала изучения дисциплины студент должен:

- знать: устройство компьютера;
- уметь: пользоваться прикладными компьютерными программами;
- иметь навыки: работы на персональном компьютере;
- иметь представление: об операционной системе компьютера.

После окончания изучения дисциплины студент должен:

В результате изучения дисциплины студенты должны:

- *иметь представление о:*

- задачах построения защищенных ЭИС;
- методах криптографической защиты;
- концепции информационной безопасности;

- *знать:*

- виды угроз информационной безопасности;
- методы и средства борьбы с угрозами информационной безопасности;
- понятие политики безопасности, существующие типы политик безопасности;
- существующие стандарты информационной безопасности;

- нормативные руководящие документы, касающиеся государственной тайны;

- *уметь:*

- выполнять анализ способов нарушений информационной безопасности;

- использовать методы и средства защиты данных.

4. Место дисциплины в учебном процессе

Место «Информационной безопасности» в структуре подготовки выпускников определяется тем, что обеспечивающей дисциплиной для нее является информатика и информационные технологии в сервисе, а сопутствующими инновации в сервисе и документооборот в сервисе

Сведения об обеспечивающих, сопутствующих и обеспечиваемых дисциплинах

№	Обеспечивающие	Сопутствующие	Обеспечиваемые
1	Информатика	Инновации в сервисе	
2	Информационные технологии в сервисе	Документооборот в сервисе	

ПРОТОКОЛ №1
согласования междисциплинарных входов и выходов

Обеспечивающая дисциплина "Информатика "
Специальность 100100
Специализация все
Курс 1 Семестр 1,2 Трудоемкость 360
Факультет

Кафедра
Заведующий кафедрой
Преподаватель дисциплины
Заведующий кафедрой, на которой читается обеспечиваемая дисциплина _____(подпись)

Обеспечивающая дисциплина "Информационные технологии в сервисе"

Специальность 100100
Специализация все
Курс 2 Семестр 4 Трудоемкость 180
Факультет ГФ
Кафедра СКТ
Заведующий кафедрой
Преподаватель дисциплины
Заведующий кафедрой, на которой читается обеспечиваемая дисциплина _____(подпись)

Сопутствующая дисциплина " Инновации в сервисе ”

Специальность 100100
Специализация все
Курс 3 Семестр 6 Трудоемкость 144
Факультет ГФ
Кафедра СКТ
Заведующий кафедрой
Преподаватель дисциплины
Заведующий кафедрой, на которой читается обеспечиваемая дисциплина (подпись)

Обеспечивающая дисциплина "Документооборот в сервисе"

Специальность 100100
Специализация все
Курс 3 Семестр 6 Трудоемкость 72
Факультет ГФ
Кафедра Фил
Заведующий кафедрой
Преподаватель дисциплины
Заведующий кафедрой, на которой читается обеспечиваемая дисциплина _____(подпись)

5. Темы и содержание лекционных занятий

Тема 1. Актуальность информационной безопасности, понятия и определения.

Актуальность информационной безопасности. Национальные интересы РФ в информационной сфере и их обеспечение. Классификация

компьютерных преступлений. Способы совершения компьютерных преступлений. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet. Понятия и определения в информационной безопасности.

Тема 2. Угрозы информации.

Виды угроз информационной безопасности РФ. Источники угроз информационной безопасности РФ. Угрозы информационной безопасности для АСОИ. Удаленные атаки на интрасети.

Тема 3. Вредоносные программы.

Условия существования вредоносных программ. Классические компьютерные вирусы. Сетевые черви. Троянские программы. Спам. Хакерские утилиты и прочие вредоносные программы. Кто и почему создает вредоносные программы.

Тема 4. Защита от компьютерных вирусов.

Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы.

Тема 5. Методы и средства защиты компьютерной информации.

Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта). Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите информации. Организация информационной безопасности компании. Выбор средств информационной информации. Информационное страхование.

Тема 6. Криптографические методы информационной безопасности.

Классификация криптографических методов. Характеристики существующих шифров. Кодирование. Стеганография. Электронная

цифровая подпись.

Тема 7. Лицензирование и сертификация в области защиты информации.

Законодательство в области лицензирования и сертификации. Правила функционирования системы лицензирования.

Тема 8. Критерии безопасности компьютерных систем.

Стандарты безопасности. Критерии безопасности компьютерных систем «Оранжевая книга». Руководящие документы Гостехкомиссии.

№ раздела подраздела, пункта подпункта	Содержание		Количество часов						
			Аудиторная работа					Самостоятельная работа	Рекомен
			Очное обучение	Заочное обучение	Вечернее отделение	Очное обучение	Заочное обучение	Вечернее отделение	
1	2		3	4	5	6	7	8	9
1	Актуальность информационной безопасности, понятия и определения	ОК12 ОК13 ОК14 ПК7 ПК12 ПК13	4						[1,5,8]
2	Угрозы информации	ОК2 ОК12 ОК13 ОК14 ПК7 ПК12 ПК13	4						[2,3,7,10,8]
3	Вредоносные программы	ОК2 ОК12 ОК13 ОК14 ПК7 ПК12 ПК13	4						[1,4,8]
4	Защита от компьютерных вирусов	ОК2 ОК12 ОК13 ОК14 ПК7 ПК12 ПК13	4						[1,3,5,9,11]
5	Методы и средства защиты компьютерной информации	ОК2 ОК12 ОК13 ОК14 ПК7 ПК12 ПК13	4						[2,6,5,9,8]
6	Криптографические методы информационной безопасности	ОК2 ОК12 ОК13 ОК14 ПК7 ПК12 ПК13	4						[1,4,6,8,12]

7	Лицензирование и сертификация в области защиты информации	ОК12 ОК13 ОК14 ПК7 ПК12 ПК13	4						[1,4]
8	Критерии безопасности компьютерных систем	ОК12 ОК13 ОК14 ПК7 ПК12 ПК13	4						[2,3,6,8]
9	Информационная безопасность на предприятиях сервиса	ОК12 ОК13 ОК14 ПК7 ПК12 ПК13	8						[1,3,5,8]
Всего по разделам		40							
Итого		40							

6. График, темы и содержание практических занятий

1. Угрозы и риски информационной безопасности (ИБ). Классификация угроз. Анализ современной статистики угроз. Реальный масштаб рисков ИБ. Возможные последствия внешних атак и действий инсайдеров. Основные каналы утечки информации.

2. Анализ рисков нарушения информационной безопасности. Выбор методики оценки рисков ИБ. Оценка рисков и возможные стратегии реагирования. Оценка экономической эффективности предполагаемых мер защиты.

3. Защита персональных данных. Разработки модели угроз и модели нарушителя. Возможные каналы утечки персональных данных. Требования к средствам защиты. Практические рекомендации по защите персональнбых данных.

4. Организационные меры обеспечения информационной безопасности. Разработка политики информационной безопасности в организации. Построение комплексной системы защиты информации в свете требований стандарта ISO 27001.

5. Технические и программные средства обеспечения информационной безопасности компании. Обзор средств защиты

информации, критерии выбора, сравнительная оценка. Практика внедрения средств защиты, возможные проблемы и пути их решения.

6. Построение корпоративной инфраструктуры открытых ключей (PKI). Средства защиты информации в каналах связи. Обеспечение безопасности данных в локальных сетях. Организация защищенного удаленного доступа и VPN. Средства защиты беспроводных сетей.

7. Средства защиты информации на рабочих станциях. Средства строгой аутентификации и разграничения доступа к ресурсам станции. Средства предотвращения утечек информации, ограничение использования сменных носителей данных и беспроводных сетей. Криптографическая защита данных на локальных дисках.

8. Средства защиты электронной почты. Использования электронно-цифровой подписи и шифрования сообщений. Средства борьбы с нежелательными сообщениями. Средства централизованного архивирования и мониторинга электронной почты.

9. Системы централизованного управления учетными записями и правами доступа на основании корпоративной политики ИБ. Управление учетными записями пользователей. Обеспечение однократной аутентификации и управление паролями.

10. Средства управления доступом при работе с Интернет. Средства разграничения доступа к интернет-ресурсам из локальной сети предприятия на основе принятых политик ИБ. Средства разграничения доступа из Интернет к ресурсам и службам организации для различных категорий пользователей.

№	неделя	Наименование практических занятий	Кол. часов			
			Очное	Заочное	вечернее обучение	Рекомендуемая литература

1	30	Угрозы и риски информационной безопасности	6			[1,3,5,8]
2	31	Анализ рисков нарушения информационной безопасности	6			[2,3,7,10,8]
3	32-33	Защита персональных данных	6			[1,4,8]
4	34-35	Организационные меры обеспечения информационной безопасности. Разработка политики информационной безопасности в организации	6			[1,3,5,9,11]
5	36-37	Технические и программные средства обеспечения информационной безопасности компании	8			[2,6,5,9,8]
6	38-39	Построение корпоративной инфраструктуры открытых ключей (PKI). Средства защиты информации в каналах связи	8			[1,4,6,8,12]
7	30-32	Средства защиты информации на рабочих станциях	6			[1,4]
8	32-34	Средства защиты электронной почты	6			[2,3,6,8]
9	34-36	Системы централизованного управления учетными записями и правами доступа на основании корпоративной политики ИБ	8			[1,3,5,8]
10	36-38	Средства управления доступом при работе с Интернет	8			[2,3,7,10,8]
Итого			68			

7. График самостоятельной работы студентов

Перечень самостоятельной работы студентов
Самостоятельная работа студентов заключается в подготовке к семинарским занятиям в объёме 108 часов. Текущий контроль результативности учебного процесса осуществляется на семинарских занятиях и промежуточных аттестаций в течение семестра. Итоговый контроль - зачет.

Вид работы	Содержание работы	Час	Учебно-методическое обеспечение
Доклад	Написание доклада по теме дисциплины	36	[1,3,5,8]
Решение задач	Решение задач по заданным параметрам	36	[2,3,7,10,8]
Проведение сравнительного анализа изученных антивирусных программных продуктов	заполнение таблиц в целях выявления достоинств и недостатком программных продуктов	36	[1,4,8]

Для обеспечения успешной самостоятельной работы студентов планируется проведение еженедельных консультаций в часы, свободные от занятий.

В качестве мотивации самостоятельной работы студентов может выступать высокий балл за выполненное задание или доклад.

Задание на выполнение самостоятельной работы:

1. Подготовка доклада

Этапы выполнения самостоятельной работы:

1. Определить цель и задачи доклада.
2. Выбрать вид, тему и название доклада.
3. Отобрать и кратко прорецензировать литературу.
4. Написать доклад на основе изученной литературы

Объем доклада должен быть 15-20 листов формата А4. Все страницы должны быть пронумерованы и скреплены. На титульном листе и на второй страницах номера не ставятся. (темы докладов в Приложении 4)

2. Решение задач

Студенту выдаются условия задачи, согласно варианту, который определяется по списку студентов для самостоятельного решения.

Рекомендации по решению и условия в прил.3

3. Проведение сравнительного анализа изученных антивирусных программных продуктов

Студент выбирает два программных продукта и сравнивает их по следующим критериям:

- удобство интерфейса;
- функции;
- стыковка с другими программными продуктами
- охват предприятий (география использования продукта);
- минусы и плюсы;

8. График контрольных мероприятий

Контроль результативности учебного процесса

Вид контроля результативности учебного процесса	Форма контроля	Средства контроля	График
1 .Входящий	Опрос	Контрольные вопросы	1-е занятие
2. Текущий или *Промежуточный*	Устный опрос Проверка практических заданий Доклад	Контрольные вопросы Задачи Темы докладов	На каждом занятии Лабораторные занятия Лабораторные занятия
3. Итоговый	Зачет		Последнее занятие

Лист контрольных мероприятий
(для выдачи обучающемуся)

Максимально возможный балл по виду учебной работы											
Перечень и содержание модуля учебной дисциплины	Текущая аттестация							Контрольное мероприятие			Итого
	Посещение лекций	Выполнение практического задания	Выполнение домашних заданий	конспекты	Контрольное мероприятие (тестирование	Работа над эссе	Активность на занятиях	Максимальный балл	экзамен	Защита курсовой работы/проекта	
Актуальность информационной безопасности, понятия и определения	0,2-0,4	0,2-0,4	0,4	0,2	0,5-1,5	0,5	0,2-1,2	4,6			
Угрозы информации	0,2-0,4	0,2-0,6	0,2	0,2			0,2-1,2	2,6			
Вредоносные программы	0,2	0,2-0,6	0,2	0,2			0,2-1,2	2,4			
Защита от компьютерных вирусов	0,2	0,2- 0,4	0,2	0,2		0,5	0,2-1,2	2,7			
Методы и средства защиты компьютерной информации	0,2	0,2-0,6	0,2	0,2			0,2-1,2	2,4			
Криптографические методы информационной безопасности	0,2	0,2-0,4	0,2	0,2	0,5-1,5		0,2-1,2	3,7			
Лицензирование и сертификация в области защиты информации	0,2-0,6	0,2-0,6	0,2	0,2		0,5	0,2-1,8	3,9			
Критерии безопасности компьютерных систем	0,2-0,6	0,2-0,6	0,2	0,2		0,5	0,2-1,8	3,9			
Информационная безопасность на предприятиях сервиса	0,2	0,5	0,2	0,2	0,5-1,5		0,2-1,2	3,8			
Обязательный минимум для допуска к экзамену	1-3	1,8 – 4,7	1-2	1-1,8	1,3-4,5	0,5-2	1-12	7,6-30	50-100		100 – 130

Посещаемость аудиторных занятий оценивается: каждое занятие – 0,2 балла:

100% -3 баллов , 99-95% -2,8 баллов, 94-90% -2,6баллов, 89-85% -2,4 баллов, 84-80% - 2,2баллов, 79-75%-2 баллов, 74-70% - 1,8баллов, 69-65% - 1,6баллов, 64-60% -1,4баллов, 59-55% - 1,2баллов, 54-50% - 1 баллов. При посещении студентом менее 50 % аудиторных занятий баллы за посещаемость не начисляются.

Выполнение практических и домашних творческих заданий. Оценивается от 0,2-0,6 баллов (творческий рейтинг):

домашние творческие задания: (презентации, слайды, коллажи, кроссворды и др.)- 0,2-,04 баллов (0,2 б. - сообщение раскрывающее тематику доклада, 0,4- сообщение подкреплено визуально: рисунки, фото, репродукции)

Активность на занятиях

Активность определяется в процессе текущего контроля, включающего разнообразные формы (устные и письменные ответы, на практических занятиях, участие в дискуссиях, рефераты, доклады и т.д.), и определяется 0,2-1,8 баллами.

Для допуска к итоговому контролю (зачет) студент должен набрать от 7,6-30 баллов. При получении максимальной рейтинга (30 баллов) по итогам посещаемости, творческого рейтинга, выполнения всех форм заданий студенту автоматически начисляются 40 баллов за зачет и выставляется оценка зачтено.

Конспекты

Каждый конспект лекции оценивается на 0,2 балла

Контрольные мероприятия

Текущее контрольное мероприятие (тестирование) оценивается от 0,5до 1,5 б. в зависимости от % правильно выполненных заданий: 1,5 б.– 100%, 1 б.- 75%,0,5 б.- 5-% заданий

Матрица контроля текущей и итоговой результативности учебного процесса по дисциплине: «Информационная безопасность»

№ раздела	Наименование раздела	Вид и форма учебных занятий, вид, метод и средство контроля						
		аудиторные			**Самостоятельные**			
		лекции	практич. занятия		Дом. задания		Творческие зад.	
		текущ	текущ	итог	текущ	итог	текущ	Итог
		Конт.посещ	Конт.посещ	Тестир	Конт.графи	Защита	Конт.график	Защита
1	Актуальность информационной безопасности, понятия и определения	Бланк уч.	Бланк уч.	Тест	Бланк уч		-	-
2	Угрозы информации	Бланк уч.	Бланк уч.	Тест	- Бланк уч	-	Бланк уч.	
3	Вредоносные программы	Бланк уч.	Бланк уч.	Тест	Бланк уч.		Бланк уч.	
4	Защита от компьютерных вирусов	Бланк уч.	Бланк уч.	Тест	Бланк уч	-	Бланк уч.	
5	Методы и средства защиты компьютерной информации	Бланк уч.	Бланк уч.	Тест	Бланк уч		Бланк уч.	
6	Криптографические методы информационной безопасности	Бланк уч.	Бланк уч.	Тест	Бланк уч		Бланк уч.	
7	Лицензирование и сертификация в области защиты информации	Бланк уч.	Бланк уч.	Тест	Бланк уч		Бланк уч.	
8	Критерии безопасности компьютерных систем	Бланк уч.	Бланк уч.	Тест	Бланк уч		Бланк уч.	
9	Информационная безопасность на предприятиях сервиса	Бланк уч.	Бланк уч.	Тест	Бланк уч		Бланк уч.	

9. Учебно-методическое обеспечение дисциплины

Основная литература.

1. Мельников В.П. Информационная безопасность: 3е издание – М: Издательский центр «Академия», 2008
2. Мельников В. П. Информационная безопасность и защита информации: учебное пособие для студентов вузов, под ред. С. А. Клейменова. - 5-е изд., стер. - М. : Академия, 2011. - 336 с

Дополнительная литература.

1. Трублина И.Т./Автоматизированные информационные технологии в экономике/М.: Финансы и статистика, 2003/1-3глава
2. Фролов К.В. и др./Безопасность России/ МГФ «Знание», 2005/1-5 глава
3. Милославская Н.Г., Толстой А.И./Интрасети: доступ в Internet, защита/М.: Радио и связь, 2000/ 1-3 глава
4. Проскурин В.Г., Крутов С.В./Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах./М.: Радио и связь, 2000/1-2 глава
5. Садердинов А.А., Трайнев В.А., Федулов А.А./Информационная безопасность предприятия/Издательский дом «Дашков и К»/2-4 глава
6. Герасименко В.А., Малюк А.А./Основы защиты информации/ ППО «Известия», 2003/ 2-8 глава
7. Мельник В.И./Защита информации в компьютерных системах/ Финансы и статистика, 2002/1-2 раздел
8. Белкин П.Ю./Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных/ М.: Радио и связь, 2004/1,2,5 глава
9. Касперский В.Е./Компьютерные вирусы:что это такое и как с ними бороться/СК Пресс, 2001/1-3 глава

10. Фролов А.В., Фролов Г.В./Осторожно: компьютерные вирусы/Диалог-МИФИ, 2004/1-2 глава

11. Горбатов В.С., Фатьянов А.А./Правовые основы защиты информации/МИФИ, 2002/1 глава

12. О сертификации продукции и услуг/ Закон Российской Федерации

13. О федеральных органах правительственной связи и информации/ Закон Российской Федерации

14. О государственной тайне/ Закон Российской Федерации

15. Об информации, информатизации и защите информации/ Закон Российской Федерации

16. О лицензировании отдельных видов деятельности/Постановление Правительства РФ

17. О сертификации средств защиты информации/ Постановление Правительства РФ

18. Руководящий документ «Защита от несанкционированного доступа к информации, термины и определения»/ Гостехкомиссия России

19. Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»/ Гостехкомиссия России

20. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»/ Гостехкомиссия России

21. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»/ Гостехкомиссия России

22. Руководящий документ «Временное положение по организации разработки, изготовления и эксплуатации программных и технических

средств защиты секретной информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники» Гостехкомиссия России

Учебно-методическое обеспечение дисциплины

№ п/п	Автор, наименование	Год издания	Количество экземпляров в научной библиотеке	Количество обучающихся	Коэффициент книгообеспеченности
	Основная литература				
1	Мельников В. П. Информационная безопасность и защита информации: учебное пособие для студентов вузов, под ред. С. А. Клейменова. - 5-е изд., стер. - М. : Академия, 2011. - 336 с	*2011.*	13	36	2,9
2	Мельников В.П. Информационная безопасность: 3е издание – М: Издательский центр «Академия», 2008	*2008*	1	36	0.02

Приложение 1

Вопросы к зачету

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.

4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
6. Понятие политики безопасности информационных систем. Назначение политики безопасности.
7. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
8. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
9. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
10. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
11. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
12. Основные положения руководящих документов Гостехкомиссии России. Классификация автоматизированных систем по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
13. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
14. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
15. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
16. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
17. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
18. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
19. Биометрические средства идентификации и аутентификации пользователей.
20. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
21. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
22. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.

23. Законодательный уровень применения цифровой подписи.
24. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
25. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
26. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
27. Средства обеспечения информационной безопасности в ОС Windows'2000. Разграничение доступа к данным. Групповая политика.
28. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows NT/2000/XP. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.
29. Применение средств Windows 2000/XP для предотвращения угроз раскрытия конфиденциальности данных. Шифрование данных. Функции и назначение EFS.
30. Разграничение доступа к данным в ОС семейства UNIX.
31. Пользователи и группы в ОС UNIX.
32. Пользователи и группы в ОС Windows'2000.
33. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
34. Причины нарушения безопасности информации при ее обработке криптографическими средствами.
35. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
36. Распределенные информационные системы. Удаленные атаки на информационную систему.
37. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
38. Физические средства обеспечения информационной безопасности.
39. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
40. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
41. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
42. Виртуальные частные сети, их функции и назначение.

Приложение 2

Вопросы для самопроверки усвоенного материала

Тема 1. Актуальность информационной безопасности, понятия и определения.

1. Особенностями современных информационных технологий?
2. Когда появились первые преступления с использованием компьютерной техники в России?
3. Сколько уголовных дела по ст.272 УК РФ («Неправомерный доступ к компьютерной информации») и ст.165 УК РФ ("Причинение имущественного ущерба путем обмана и злоупотребления доверием") было возбуждено в 2003 году в России?
4. Какой ущерб нанесли компьютерные вирусы за последние 5 лет?
5. Что понимается под информационной безопасностью Российской Федерации?
6. Первая составляющая национальных интересов Российской Федерации в информационной сфере?
7. Вторая составляющая национальных интересов Российской Федерации в информационной сфере?
8. Третья составляющая национальных интересов Российской Федерации в информационной сфере?
9. Четвертая составляющая национальных интересов Российской Федерации в информационной сфере?
10. Классификация компьютерных преступлений?
11. Экономические компьютерные преступления?
12. Компьютерными преступлениями против личных прав и частной сферы?
13. Компьютерные преступления против государственных и общественных интересов?
14. Основные виды преступлений, связанных с вмешательством в работу компьютеров?
15. Способы совершения компьютерных преступлений?
16. Методы перехвата компьютерной информации?
17. Пользователи и злоумышленники в Internet?
18. Кто такие хакеры?
19. Кто такие фракеры?
20. Кто такие кракеры?
21. Кто такие фишеры?
22. Кто такие скамеры?
23. Кто такие спамеры?

24. Причины уязвимости сети Internet?
25. Защищаемая информация это?
26. Защита информации это?
27. Защита информации от утечки это?
28. Защита информации от несанкционированного воздействия это?
29. Защита информации от непреднамеренного воздействия это?
30. Защита информации от разглашения это?
31. Защита информации от несанкционированного доступа это?
32. Защита информации от иностранной разведки это?
33. Защита информации от иностранной технической разведки это?
34. Защита информации от агентурной разведки это?
35. Цель защиты информации?
36. Эффективность защиты информации это?
37. Показатель эффективности защиты информации это?
38. Нормы эффективности защиты информации это?
39. Организация защиты информации это?
40. Система защиты информации это?
41. Мероприятие по защите информации это?
42. Мероприятие по контролю эффективности защиты информации это?
43. Техника защиты информации это?
44. Объект защиты это?
45. Способ защиты информации это?
46. Категорирование защищаемой информации это?
47. Метод контроля эффективности защиты информации это?
48. Контроль состояния защиты информации это?
49. Средство защиты информации это?
50. Средство контроля эффективности защиты информации это?
51. Контроль организации защиты информации это?
52. Контроль эффективности защиты информации это?
53. Организационный контроль эффективности защиты информации это?
54. Технический контроль эффективности защиты информации это?
55. Информация это?
56. Доступ к информации это?
57. Субъект доступа к информации это?
58. Носитель информации это?
59. Собственник информации это?
60. Владелец информации это?
61. Пользователь (потребитель) информации это?
62. Право доступа к информации это?
63. Правило доступа к информации это?
64. Орган защиты информации это?
65. Информационные процессы это?

66. Информационная система это?
67. Информационными ресурсами это?
68. Что понимают под утечкой информации?
69. Несанкционированный доступ это?
70. Несанкционированное воздействие это?
71. Что понимается под непреднамеренным воздействием на защищенную информацию?
72. Что понимается под эффективностью защиты информации?
73. Конфиденциальность информации это?
74. Шифрование информации это?
75. Уязвимость информации это?

Тема 2. Угрозы информации.

1. Виды угроз информационной безопасности Российской Федерации?
2. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности?
3. Угрозы информационному обеспечению государственной политики Российской Федерации?
4. Угрозы развитию отечественной индустрии информации?
5. Угрозы безопасности информационных и телекоммуникационных средств и систем?
6. Источники угроз информационной безопасности Российской Федерации?
7. К внешним источникам информационной безопасности Российской Федерации относятся?
8. К внутренним источникам информационной безопасности Российской Федерации относятся?
9. Угрозы информационной безопасности для автоматизированных систем обработки информации (АСОИ)?
10. Уязвимость основных структурно-функциональных элементов распределенных АСОИ?
11. Основные виды угроз безопасности субъектов информационных отношений?
12. Классификация угроз безопасности информации?
13. Естественные угрозы информации это?
14. Искусственные угрозы информации это?
15. Непреднамеренные угрозы информации это?
16. Преднамеренные угрозы информации это?
17. Основные непреднамеренные искусственные угрозы?
18. Основные преднамеренные искусственные угрозы?
19. Классификация каналов проникновения в систему и утечки информации?
20. Неформальная модель нарушителя в АС?
21. Удаленные атаки на интрасети?

22. Что принято понимать под удаленной атакой?
23. Классификация удаленных атак?

Тема 3. Вредоносные программы.

1. Какие программы являются вредоносными?
2. Условия существования вредоносных программ?
3. Причины появления вредных программ?
4. Классические компьютерные вирусы?
5. Классификация классических вирусов?
6. Способы заражения компьютерными вирусами?
7. Внедрение вируса в начало файла?
8. Внедрение вируса в конец файла?
9. Внедрение вируса в середину файла?
10. Вирусы без точки входа?
11. Загрузочные вирусы?
12. Макровирусы?
13. Сетевые черви?
14. Классификация сетевых червей?
15. Email-Worm – почтовые черви?
16. IM-Worm – черви, использующие интернет-пейджеры?
17. IRC-Worm – черви в IRC-каналах?
18. Net-Worm – прочие сетевые черви?
19. P2P-Worm – черви для файлообменных сетей?
20. Троянские программы?
21. Классификация троянских программ?
22. Backdoor – троянские утилиты удаленного администрирования?
23. Trojan-PSW – воровство паролей?
24. Trojan-Clicker – интернет-кликеры?
25. Trojan-Downloader – доставка вредоносных программ?
26. Trojan-Dropper – инсталляторы вредоносных программ?
27. Trojan-Proxy – троянские прокси-сервера?
28. Trojan-Spy – шпионские программы?
29. Trojan – прочие троянские программы?
30. Rootkit – сокрытие присутствия в операционной системе?
31. ArcBomb – «бомбы» в архивах?
32. Trojan-Notifier – оповещение об успешной атаке?
33. Спам?
34. Основные виды спама?
35. Хакерские утилиты и прочие вредоносные программы?
36. Основные виды хакерских утилит и прочих вредоносных программ?
37. DOS, DDOS – сетевые атаки?
38. Exploit, HackTool – взломщики удаленных компьютеров?
39. Flooder – «замусоривание» сети?
40. Constructor – конструкторы вирусов и троянских программ?
41. Nuker – фатальные сетевые атаки?

42. Bad-Joke, Hoax – злые шутки, введение пользователя в заблуждение?
43. FileCryptor, PolyCryptor – скрытие от антивирусных программ?
44. PolyEngine – полиморфные генераторы?
45. Кто и почему создает вредоносные программы?

Тема 4. Защита от компьютерных вирусов.

1. Признаки заражения компьютера?
2. Косвенные признаки заражения компьютера?
3. Действия при появлении признаков заражения вредоносной программой?
4. Источники компьютерных вирусов?
5. Глобальные сети и электронная почта как источник компьютерных вирусов?
6. Электронные конференции как источник компьютерных вирусов?
7. Локальные сети как источник компьютерных вирусов?
8. Пиратское программное обеспечение как источник компьютерных вирусов?
9. Компьютеры общего пользования как источник компьютерных вирусов?
10. Ремонтные службы как источник компьютерных вирусов?
11. Основные правила защиты от компьютерных вирусов?
12. Антивирусные программы?
13. Виды антивирусных программ?
14. Типовой перечень функций, которые способны выполнять антивирусные программы?
15. К наиболее мощным и популярным на сегодняшний день в России антивирусным пакетам относятся?
16. Принцип работы антивирусного сканера?
17. Принцип работы антивирусных программ-детекторов?
18. Принцип работы антивирусных программ-докторов (фагов)?
19. Принцип работы антивирусных программ-ревизоров?
20. Принцип работы антивирусных программ-фильтров (сторожей)?
21. Принцип работы вакцинаторов (иммунизаторов)?

Тема 5. Методы и средства защиты компьютерной информации.

1. Методы обеспечения информационной безопасности Российской Федерации?
2. Правовые методы обеспечения информационной безопасности Российской Федерации?
3. Организационно – техническими методами обеспечения информационной безопасности Российской Федерации?
4. Экономические методы обеспечения информационной безопасности Российской Федерации?
5. Основные меры по обеспечению информационной безопасности Российской Федерации в сфере экономики?

6. Наиболее важные объекты обеспечения информационной безопасности Российской Федерации в области науки и техники?
7. Ограничение доступа как метод обеспечения информационной безопасности?
8. Биометрические методы аутентификации человека?
9. Статистика применения биометрических технологий?
10. Отпечатки пальцев как биометрическая характеристика идентификации человека?
11. Глаза как биометрическая характеристика идентификации человека?
12. Лицо как биометрическая характеристика идентификации человека?
13. Ладонь как биометрическая характеристика идентификации человека?
14. Динамические характеристики как биометрическая характеристика идентификации человека?
15. Классификация систем тревожной сигнализации?
16. Контроль доступа к аппаратуре как метод обеспечения информационной безопасности?
17. Разграничение и контроль доступа к информации как метод обеспечения информационной безопасности?
18. Предоставление привилегий на доступ как метод обеспечения информационной безопасности?
19. Идентификация и установление подлинности объекта (субъекта)?
20. Объекты идентификации и установления подлинности в АСОИ?
21. Идентификация и установление подлинности личности?
22. Идентификация и установление подлинности технических средств?
23. Идентификация и установление подлинности документов?
24. Идентификация и установление подлинности информации на средствах ее отображения и печати?
25. Защита информации от утечки за счет побочного электромагнитного излучения и наводок?
26. Методы и средства защиты информации от побочного электромагнитного излучения и наводок информации?
27. Методы и средства защиты информации от случайных воздействий?
28. Методы защиты информации от аварийных ситуаций?
29. Организационные мероприятия по защите информации?
30. Организация информационной безопасности компании?
31. Выбор средств информационной информации?
32. Информационное страхование?

Тема 6. Криптографические методы информационной безопасности.

1. Криптографические методы информационной безопасности?

2. Классификация методов криптографического закрытия информации?
3. Чем занимается наука криптология?
4. Что такое криптоанализ?
5. Стойкость криптографического метода это?
6. Трудоемкость криптографического метода это?
7. Основные требования к криптографическому закрытию информации?
8. Шифрование это?
9. Классификация криптосистем?
10. Симметричные криптосистемы?
11. Классификация симметричных криптосистем?
12. Шифрование методом замены (подстановки)?
13. Одноалфавитная подстановка?
14. Многоалфавитная одноконтурная обыкновенная подстановка?
15. Многоалфавитная одноконтурная монофоническая подстановка?
16. Многоалфавитная многоконтурная подстановка?
17. Шифрование методом перестановки?
18. Шифрование методом гаммирования?
19. Шифрование с помощью аналитических преобразований?
20. Комбинированные методы шифрования?
21. Криптосистемы с открытым ключом (асимметричные)?
22. Характеристики существующих шифров?
23. Кодирование это?
24. Стеганография это?
25. Основные правила криптозащиты?
26. Основные правилами механизма распределения ключей?
27. Электронная цифровая подпись?
28. Технология электронной цифровой подписи?
29. Электронный документ это?
30. Электронная цифровая подпись это?
31. Владелец сертификата ключа подписи это?
32. Средства электронной цифровой подписи это?
33. Сертификат средств электронной цифровой подписи это?
34. Закрытый ключ электронной цифровой подписи это?
35. Открытый ключ электронной цифровой подписи это?
36. Сертификат ключа подписи это?
37. Подтверждение подлинности электронной цифровой подписи в электронном документе это?
38. Пользователь сертификата ключа подписи это?
39. Информационная система общего пользования это?
40. Корпоративная информационная система это?

Тема 7. Лицензирование и сертификация в области защиты информации.

1. Лицензирование и сертификация в области защиты информации?

2. Законодательство в области лицензирования и сертификации?
3. Нормы и требования российского законодательства в области лицензирования и сертификации?
4. Постановление Правительства РФ № 2195-1 "О видах деятельности, которыми предприятия вправе заниматься только на основании специальных разрешений (лицензий)".
5. Закон РФ "О федеральных органах правительственной связи и информации" № 4524-1?
6. Закон Российской Федерации от 21.07.93 "О государственной тайне" № 5485-1?
7. Постановление Правительства РФ от 24.12.94 № 1418 "О лицензировании отдельных видов деятельности"?
8. Закон РФ "Об информации, информатизации и защите информации" от 20.02.95 № 24-ФЗ?
9. Указ Президента РФ № 334 "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации"?
10. Постановление Правительства РФ от 15 апреля 1995 года № 333 "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны"?
11. Постановление Правительства РФ от 26.06.95 № 608 "О сертификации средств защиты информации"?
12. Закон РФ "Об участии в международном информационном обмене" от 5 июня 1996 года N 85-ФЗ?
13. Какие виды деятельности подлежат лицензированию?
14. Какие средства подлежат сертификации Федеральным агентством?
15. Правила функционирования системы лицензирования?
16. В каких случаях заявителю может быть отказано в получении лицензии?
17. В каких случаях выданная лицензия может быть приостановлена или аннулирована?
18. Какие документы прилагаются к заявлению на получение лицензии?
19. Какие цели специальной экспертизы?

Тема 8. Критерии безопасности компьютерных систем.

1. Критерии безопасности компьютерных систем?
2. Оранжевая книга это?
3. Какие определены в Оранжевой книге группы фундаментальных требований?

4. Требования группы фундаментальных требований Оранжевой книги «Стратегия»?
5. Требования группы фундаментальных требований Оранжевой книги «Подотчетность»?
6. Требования группы фундаментальных требований Оранжевой книги «Гарантии»?
7. На какие группы разделяются автоматизированные системы в Оранжевой книге?
8. Краткая характеристика классов в Оранжевой книге?
9. Основным недостаткам Оранжевой книги?
10. Какие руководящие документы Гостехкомиссии?
11. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»?

Приложение 3

Задание для самостоятельной работы

Задачи по анализу стойкости функций безопасности

Важным моментом при оценке объекта оценки на соответствие требованиям задания по безопасности в соответствии с ГОСТ Р ИСО/МЭК 15408 является анализ уязвимостей и стойкости функций безопасности. Цель обоих видов проверки заключается в выявлении степени устойчивости ОО по отношению к нападениям, выполняемых нарушителем с определенным (низким, умеренным или высоким) потенциалом нападения.

Анализ уязвимостей применяется по всем функциям безопасности. При этом не делается, каких-либо предположений относительно корректности их реализации, сохранения целостности, возможности обхода и т.п.

Анализу стойкости подвергаются только функции безопасности, реализованные с помощью вероятностных или перестановочных механизмов, у которых и проверяется стойкость (базовая, средняя или высокая). Базовая – означает защищенность от источника угрозы с низким потенциалом нападения.

В принципе, все вероятностные функции можно считать уязвимыми, а подобный анализ, классифицировать как анализ уязвимостей специального вида. Для успешного нападения надо сначала идентифицировать, а затем использовать некоторую уязвимость.

Оба действия оцениваются с точки зрения временных затрат, необходимой квалификацией, уровня знаний об ОО, характере и продолжительности доступа к ОО, необходимых аппаратно - программных и иных ресурсов.

Все эти составляющие не являются независимыми. Высокая квалификация может сэкономить время, а специальное оборудование упростить и ускорить доступ к ОО, следовательно, если оценивать каждый параметр количественно, то результирующую функцию, характеризующую серьезность уязвимости естественно сделать аддитивной.

В таблицах содержатся условные баллы, присваиваемые параметрам уязвимостей в зависимости от того, в какой диапазон или на какой уровень они попадают. Для получения общего рейтинга нужно выбрать по одному значению из обоих числовых столбцов всех таблиц и сложить эти десять чисел.

При оценке стойкости функций безопасности, фаза идентификации не рассматривается (предполагается, что уязвимость известна), поэтому достаточно выбрать и сложить пять чисел из последних столбцов.

Таблица 1 - Условные баллы, присваиваемые уязвимости в зависимости от времени на ее идентификацию и использование

Диапазон	**Идентификация уязвимости**	**Использование уязвимости**
Меньше 0,5 часа	0	0
Меньше суток	2	3
Меньше месяца	3	5
Больше месяца	5	8

Таблица 2 - Условные баллы, присваиваемые уязвимости в зависимости от уровня квалификации для ее идентификации и использования

Уровень	**Идентификация уязвимости**	**Использование уязвимости**
Любитель	0	0
Специалист	2	2
Эксперт	5	4

Таблица 3 - Условные баллы, присваиваемые уязвимости в зависимости от уровня знаний об ОО

Уровень	**Идентификация уязвимости**	**Использование уязвимости**
Отсутствие знаний	0	0
Общедоступные знания	2	2
Конфиденциальные сведения	5	4

Таблица 4 - Условные баллы, присваиваемые уязвимости в зависимости от времени доступа к ОО

Диапазон	**Идентификация уязвимости**	**Использование уязвимости**
Меньше 0,5 часа или доступ незаметен	0	0
Меньше суток	2	4
Меньше месяца	3	6
Больше месяца	4	9

Таблица 5 - Условные баллы, присваиваемые уязвимости в зависимости от аппаратно-программных и иных ресурсов (оборудования), необходимых для ее идентификации и использования

Уровень	**Идентификация уязвимости**	**Использование уязвимости**
Отсутствие	0	0

оборудования		
Стандартное оборудование	1	2
Специальное оборудование	3	4
Заказное оборудование	5	6

Если уязвимость можно идентифицировать и/или использовать различными методами, для каждого из них вычисляется рейтинг и из полученных значений выбирается минимальное, то есть уязвимость характеризуется самым простым методом успешного нападения.

В таблице **Ошибка! Закладка не определена.** приведены диапазоны рейтинга, характеризующие стойкость функций безопасности.

Таблица 6 - Диапазоны рейтинга, характеризующие стойкость функций безопасности

Диапазон	**Стойкость функций безопасности**
10 - 17	Базовая
18 - 24	Средняя
более 24	Высокая

Согласно общей методологии, потенциал нападения оценивается, в общем и целом по той же схеме, что и степень риска от наличия уязвимостей с некоторыми очевидными отличиями (например, из нескольких сценариев нападения выбирается худший с наибольшим потенциалом). Считается, что он является функцией уровня мотивации злоумышленника, его квалификации и имеющихся ресурсов.

Мотивация влияет на выделяемые на нападение время и, возможно, на привлекаемые ресурсы и подбор нападающих.

В таблице **Ошибка! Закладка не определена.** приведены диапазоны рейтинга, иллюстрирующие определенный потенциал нападения.

Таблица 7 - Диапазоны рейтинга, характеризующие потенциал нападения

Диапазон	**Потенциал нападения**
меньше 10	Низкий
10 - 17	Умеренный
18 - 24	Высокий
более 24	Нереально высокий

Нападение может быть успешным, только если его потенциал не меньше рейтинга уязвимости. Отсюда следует, в частности, что уязвимости с рейтингом выше 24 устойчивы к нападению с высоким потенциалом, поэтому их практическое использование злоумышленником представляется нереальным.

Потенциал предполагаемых нападений на ОО выявляется дважды:

– при анализе ЗБ для выбора надлежащих мер противодействий;

– при анализе уязвимостей для определения достаточности выбранных мер и качества их реализации.

Рассмотрим пример анализа стойкости функций безопасности.

Пусть доступ к ИС осуществляется посредством территориально разнесенных терминалов, работа за которыми не контролируется.

Авторизованные пользователи проходят аутентификацию путем введения паролей, состоящих из пяти десятичных чисел. Если пароль введен неверно, терминал блокируется на десять секунд. Требуется оценить стойкость такой парольной защиты для заданного пользователя с известным нападающему входным именем. Для нападения выбран один терминал.

Число возможных последовательностей является числом размещений с повторениями и составляет в данном случае: 10^5

$$П = A^d \qquad (1)$$

где А – число символов алфавита.

Ожидаемое время успешного подбора пароля методом полного перебора (Тц) оценивается полупроизведением числа возможных паролей и времени, требуемого для того, чтобы попробовать каждый пароль из последовательности:

$$A^d * \frac{t}{2} \qquad (2)$$

где t – время, требуемое на одну попытку введения пароля. Оно в общем случае равно:

$$t = \frac{k}{v} \qquad (3)$$

где v – скорость передачи сообщений с паролем (в символах/в минуту);

k – количество символов, в передаваемом сообщении при попытке получить доступ (включая пароль и служебные символы).

Если k=6, то v=60 символов в минуту. t=6с+10с=16с, тогда Тц=100000*8=800000=13300 минут=220 часов.

Это больше суток, меньше месяца, никакой квалификации и знаний или оборудования для этого не нужно. Следовательно, чтобы определить стойкость функции достаточно сложить два числа: 5-из первой таблицы и 6-из четвертой таблицы. Сумма 11 позволяет сделать вывод, что данная функция безопасности при сделанных допущениях относительно скорости передачи и количества служебных символов, обладает базовой стойкостью и является устойчивой к нападению с низким потенциалом.

Типовая задача:

Оценить устойчивость механизма парольной защиты при длине пароля d, величине алфавита А, количестве символов в сообщении при вводе пароля K, скорости ввода сообщения с паролем V к нападению нарушителя с определенным потенциалом нападения, характеризуемым уровнем квалификации (У), знаний (З) и ресурсов (Р).

Варианты заданий по теме 1

1	Условия типовой задачи: A=36 d=4 K=5 V=60 У-любитель З-отсутствие Р - отсутствие
2	Условия типовой задачи: A=36 d=5 K=6 V=60 У-любитель З-отсутствие Р - отсутствие
3	Условия типовой задачи: A=36 d=6 K=7 V=60 У-любитель З-отсутствие Р - отсутствие
4	Условия типовой задачи: A=36 d=7 K=8 V=60 У-любитель З-отсутствие Р - отсутствие
5	Условия типовой задачи: A=36 d=8 K=9 V=60 У-любитель З-отсутствие Р - отсутствие
6	Условия типовой задачи: A=26 d=4 K=5 V=60 У-любитель З-отсутствие Р - отсутствие
7	Условия типовой задачи: A=26 d=5 K=6 V=60 У-любитель З-отсутствие Р - отсутствие
8	Условия типовой задачи: A=26 d=6 K=7 V=60 У-любитель З-отсутствие Р - отсутствие
9	Условия типовой задачи: A=26 d=7 K=8 V=60 У-любитель З-отсутствие Р - отсутствие
10	Условия типовой задачи: A=26 d=8 K=9 V=60 У-любитель З-отсутствие Р - отсутствие
11	Условия типовой задачи: A=36 d=5 K=6 V=60 У-специалист З-общедоступные Р - стандартное
12	Условия типовой задачи: A=36 d=5 K=6 V=60 У-эксперт З-общедоступные Р - отсутствие
13	Условия типовой задачи: A=36 d=5 K=6 V=60 У-эксперт З-конфиденциальные Р - отсутствие
14	Условия типовой задачи: A=36 d=5 K=6 V=60 У-специалист З-конфиденциальные Р -стандартное
15	Условия типовой задачи: A=10 d=8 K=9 V=60 У-любитель З-отсутствие Р - отсутствие
16	Условия типовой задачи: A=2 d=8 K=9 V=60 У-любитель З-отсутствие Р - отсутствие
17	Условия типовой задачи: A=46 d=5 K=6 V=60 У-любитель З-отсутствие Р - отсутствие
18	Условия типовой задачи: A=46 d=5 K=6 V=60 У-специалист З-отсутствие Р - отсутствие
19	Условия типовой задачи: A=46 d=8K=9 V=60 У-любитель З-отсутствие Р - отсутствие
20	Условия типовой задачи: A=46 d=4 K=5 V=60 У-специалист З-отсутствие Р - отсутствие
21	Условия типовой задачи: A=46 d=6 K=7 V=60 У-специалист З-отсутствие Р - отсутствие
22	Условия типовой задачи: A=46 d=7 K=8 V=60 У-специалист З-отсутствие Р - отсутствие

23	Условия типовой задачи: A=36 d=8 K=9 V=50 У-любитель З-отсутствие Р - отсутствие
24	Условия типовой задачи: A=36 d=8 K=9 V=55 У-любитель З-отсутствие Р - отсутствие
25	Условия типовой задачи: A=36 d=8 K=9 V=65 У-любитель З-отсутствие Р - отсутствие
26	Условия типовой задачи: A=36 d=8 K=9 V=70 У-любитель З-отсутствие Р - отсутствие
27	Условия типовой задачи: A=36 d=8 K=9 V=75 У-любитель З-отсутствие Р - отсутствие
28	Условия типовой задачи: A=36 d=6 K=7 V=80 У-любитель З-отсутствие Р - отсутствие
29	Условия типовой задачи: A=36 d=6 K=7 V=85 У-специалист З-отсутствие Р - отсутствие
30	Условия типовой задачи: A=36 d=6 K=7 V=90 У-эксперт З-отсутствие Р - отсутствие

Приложение 4

Темы докладов

1. Сущность угрозы безопасности информации
2. Понятие угрозы безопасности информации и общие подходы к ее классификации
3. Классификация угроз безопасности информации по способам их возможного негативного воздействия
4. Нарушители безопасности информации
   Происхождение угроз безопасности информации
5. Предпосылки появления угроз
6. Основы теории защиты информации
7. Сущность теории защиты информации, ее основные составляющие и задачи
8. Моделирование процессов защиты информации
9. Стратегии защиты информации
10. Системы защиты информации
11. Понятие и структура систем защиты информации
12. Типизация и стандартизация систем защиты информации
13. Центры защиты информации и их функции
14. Роль стандартов и спецификаций в обеспечении информационной безопасности
15. Стандарты и спецификации в области информационной безопасности и их классификация
16. Общие сведения о стандартах и спецификациях в области информационной безопасности
17. «Оранжевая книга»
18. Гармонизированные критерии Европейских стран
19. Руководящие документы (РД) Гостехкомиссии России
20. X.800 «Архитектура безопасности для взаимодействия открытых систем»
21. Спецификация Internet-сообщества RFC 1510 «Сетевой сервис аутентификации Kerberos (V5)»
22. FIPS 140-2 «Требования безопасности для криптографических модулей»
23. «Обобщенный прикладной программный интерфейс службы безопасности»
24. Технические спецификации IPsec [IPsec]
25. TLS.
26. X.500 «Служба директорий: обзор концепций, моделей и сервисов»

27. Рекомендация Internet-сообщества «Руководство по информационной безопасности предприятия»
28. Рекомендация «Как выбирать поставщика Internet-услуг»
29. Британский стандарт BS 7799 «Управление информационной безопасностью. Практические правила»
30. Характеристики безопасности для различных информационных объектов
31. Операционные системы
32. Системы управления базами данных
33. Виртуальные частные сети
34. Виртуальные локальные сети
35. Обеспечение информационной безопасности в общемировых сетях
36. Спецификации Internet-сообщества IPsec
37. Архитектура средств безопасности IP-уровня
38. Контексты безопасности и управление ключами
39. Обеспечение аутентичности IP-пакетов
40. Обеспечение конфиденциальности сетевого трафика
41. Роль поставщика Internet-услуг в реагировании на нарушения безопасности
42. Меры по защите Internet-сообщества
43. Обеспечение безопасности маршрутизаторов
44. Особенности использования управляющих протоколов
45. Безопасное размещение сетевого оборудования потребителя
46. Защита системной инфраструктуры
47. Работа с Web-серверами