Федеральное агентство по образованию РФ
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ГОУВПО «АмГУ»

УТВЕРЖДАЮ
Зав. кафедрой ИУС
_____А.В. Бушманов
«___»_____

УЧЕБНО – МЕТОДИЧЕСКИЙ КОМПЛЕКС

по дисциплине «МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

для студентов специальности 230102 – Автоматизированные системы обработки информации и управления

Составитель: доцент, к.т.н. Самохвалова С.Г.

Факультет Математики и информатики

Кафедра информационных и управляющих систем

2007

Печатается по решению
редакционно-издательского совета
Факультета математики и информатики
Амурского государственного университета

С.Г. Самохвалова
Учебно-методический комплекс по дисциплине «Методы и средства защиты компьютерной информации» для студентов очной формы обучения специальности 230102 – Автоматизированные системы обработки информации и управления. - Благовещенск: Амурский гос. ун-т, 2007. – с.

Учебно-методические рекомендации ориентированы на оказание помощи студентам очной формы обучения по специальности 230102 – Автоматизированные системы обработки информации и управления для успешного освоения дисциплины «Методы и средства защиты компьютерной информации».

СОДЕРЖАНИЕ

Федеральное агентство по образованию РФ
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ГОУВПО «АмГУ»)

УТВЕРЖДАЮ

Проректор по УНР

_____ Е.С. Астапова

«___» _____ 2006 г.

РАБОЧАЯ ПРОГРАММА

По дисциплине: Методы и средства защиты компьютерной информации

Для специальности: 230102 – Автоматизированные системы обработки информации и управления

КУРС: 4 **СЕМЕСТР: 7**

ЛЕКЦИИ: 45 (ЧАС.) **ЭКЗАМЕН: 7 СЕМЕСТР**

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ: НЕТ **ЗАЧЕТ: НЕТ**

Лабораторные занятия: 30 (час.)

Самостоятельная работа: 54 (час.)

Всего часов: 129 (час.)

Составитель: Самохвалова С.Г.

Факультет Математики и информатики

Кафедра Информационных и управляющих систем

2006 г.

Рабочая программа составлена на основании Государственного образовательного стандарта ВПО по специальности 230102 – Автоматизированные системы обработки информации и управления

Рабочая программа обсуждена на заседании кафедры Информационных и управляющих систем

«___» _____ 2006 г., протокол № ___

Заведующий кафедрой А.В. Бушманов

Рабочая программа одобрена на заседании УМС 230102 – Автоматизированные системы обработки информации и управления

«___» _____ 2006 г., протокол № ___

Председатель А.В. Бушманов

Согласовано
Начальник УМУ
_____ Г.Н. Торопчина
«___» _____ 2006 г.

Согласовано
Председатель УМС факультета
_____ Е.Л. Ерёмин
«___» _____ 2006 г.

Согласовано
Заведующий выпускающей кафедрой
_____ А.В. Бушманов

«___» _____ 2006 г.

1. Цели и задачи дисциплины, ее место в учебном процессе

1.1. Цель преподавания дисциплины

Целью преподавания дисциплины является ознакомление с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации пользователей, борьбы с вирусами, изучение способов применения методов защиты информации при проектировании автоматизированных систем обработки информации и управления (АСОИУ)

1.2. Требования к уровню освоения содержания дисциплины.

В результате изучения программы курса студенты должны: знать правовые основы защиты компьютерной информации, организационные, технические и программные методы защиты информации в АСОИУ, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов; уметь применять методы защиты компьютерной информации при проектировании АСОИУ в различных предметных областях; иметь представление о направлениях развития и перспективах защиты информации.

1.3. Связь с другими дисциплинами учебного плана

Для усвоения курса необходимо знание соответствующих разделов (тем) предшествующих дисциплин учебного плана: "Операционные системы", "Информатика", "Алгоритмические языки и программирование", "Технология "программирования", "Системное программное обеспечение".

2. Содержание дисциплины

2.1. Федеральный компонент

Обще профессиональная дисциплина ГОС ВПО: 2040 ОПД – Ф.12.

2.2. Наименование тем, их содержание, объем в лекционных часах

ТЕМАТИЧЕСКИЙ ПЛАН ЛЕКЦИОННЫХ ЗАНЯТИЙ

№ темы	Наименование темы	Кол-во часов
1	Автоматизированные системы обработки данных как объекты защиты информации	4

2	Объекты защиты информации	4
3	Законодательные и правовые основы защиты компьютерной информации	3
4	Потенциальные угрозы безопасности информации в АСОД	8
5	Методы защиты информации в автоматизированных системах обработки данных	10
6	Криптографическое преобразование информации	8
7	Симметричные криптосистемы	6
8	Цифровая подпись	2
ИТОГО		**45**

Тема 1. Автоматизированные системы обработки данных как объекты защиты информации

Предмет защиты. Виды и формы представления информации. Машинное представление информации. Физическое представление информации и процессы ее обработки в АСОД. Информация как объект права собственности. Информация как коммерческая тайна.

Тема 2. Объекты защиты информации.

Классификация объектов защиты информации. Автоматизированные системы с централизованной обработкой данных. Классификация вычислительных сетей. Автоматизированные системы управления.

Тема 3. Законодательные и правовые основы защиты компьютерной информации

Нормативно-правовая база функционирования систем защиты информации. Российское законодательство по защите информационных технологий. Обзор зарубежного законодательства в области информационной безопасности.

Тема 4. Потенциальные угрозы безопасности информации в АСОД

Основные определения и критерии классификации угроз. Случайные угрозы. Преднамеренные угрозы. Вредоносное программное обеспечение.

Тема 5.. **Методы защиты информации в автоматизированных системах обработки данных**

Краткий обзор современных методов защиты информации. Ограничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации АСОД. Разделение привилегий на доступ. Идентификация и аутентификация объекта и субъекта.

Тема 6. Криптографическое преобразование информации

Краткий обзор и классификация методов шифрования информации. Классическая криптография. Примеры простых шифров Классификация криптографических методов. Криптосистема. Криптоанализ Требования к криптосистемам. Оценка криптостойкости . Выбор метода преобразования.

Тема 7. **Симметричные криптосистемы**

Основные понятия и определения. Шифры перестановки. Шифры простой замены. Блочные и потоковые шифры. Шифрование методом гаммирования . Методы генерации псевдослучайных последовательностей чисел. Американский стандарт шифрования данных DES. Основные режимы работы алгоритма DES. Режим простой замены. Режим гаммирования.

Тема 8. Цифровая подпись

Цифровая сигнатура. Хэш-функции. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля (EGSA).

2.3. Лабораторные занятия

2.3.1. Лабораторная работа 1. Оценочный расчет защищенности помещений от утечки речевых сообщений по акустическому каналу – 2 ч.

2.3.2. Лабораторная работа 2. Оценочный расчет защищенности помещений от утечки информации по электромагнитному каналу – 2 ч.

2.3.3. Лабораторная работа 3. Изучение традиционных симметричных криптосистем.Шифры перестановок – 4 ч.

2.3.4. Лабораторная работа 4. Изучение традиционных симметричных криптосистем Шифры замены – 4 ч.

2.3.5. Лабораторная работа 5. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации – 8 ч.

2.3.6. Лабораторная работа 6. Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей – 6 ч.

2.3.7. Лабораторная работа 7. Использование функций криптографического интерфейса *Windows* для защиты информации – 4 ч.

2.4. Самостоятельная работа студентов

1. Изучение материала дисциплины по конспекту лекций, учебным и справочным пособиям, методическим пособиям при подготовке к лабораторным занятиям.
2. Оформление отчетов о лабораторных работах

2.5. Вопросы к экзамену

1. Понятие ИБ. Основные составляющие ИБ и их роль при создании ИС.
2. Значение и роль ИБ в современном мире. Объектно-ориентированный подхода к ИБ.
3. Примеры объектно-ориентированного подхода к рассмотрению защищаемых ИС и недостатки традиционного подхода.
4. Угрозы ИБ (основные определения) и критерии классификации угроз.
5. Примеры угроз и рисков по всем основным составляющим (аспектам) ИБ.
6. Анализ угроз и рисков ИС с точки зрения ИБ (матрица рисков).
7. Уровни ИБ. Основные задачи и положения, решаемые на каждом уровне.

8. Российское и международное законодательство в области защиты информации.
9. Стандарты и спецификации в области защиты информации, их основные положения и принципы построения.
10. Основные механизмы и сервисы безопасности.
11. Сетевая безопасность, наиболее характерные угрозы для сетевых ИС, точки входа.
12. Административный уровень ИБ (основные понятия, политика безопасности).
13. Программа безопасности, синхронизация программы безопасности с жизненным циклом систем.
14. Управление рисками. Основные понятия, принципы, этапы.
15. Процедурный уровень ИБ, классификация мер этого уровня.
16. Принципы физической и архитектурной безопасности ИС. Иерархическая организация ИС.
17. Идентификация и аутентификация (способы, их достоинства и недостатки), управление доступом.
18. Управление доступом, технологии, принципы организации, типичные решения.
19. Технологии протоколирования и аудита. Принципы построения и задачи, зависимость от других средств ИБ, активный и пассивный аудит.
20. Использование криптографических технологий в ИС. Основные методы шифрования, сервисы безопасности, использующие криптографию.
21. Система ЭЦП. Законодательство по использованию ЭЦП и криптографических методов.
22. Межсетевые экраны, классификации, принципы работы, примеры использования в ИС.
23. Принципы работы и использование методов анализа защищённости.
24. Технические средства, обеспечивающие защиту информации, их классификация и назначение.
25. Технические средства для обнаружения устройств скрытого съема информации.
26. Технические средства для противодействия съема информации в телефонных линиях.
27. Методы и технологии защиты информации при передачи через сети общего пользования.
28. Программно-технические меры обеспечения ИБ, виды, архитектурные принципы, сервисы.
29. Цели, основные этапы и принципы действий злоумышленников, классификация типов злоумышленников.
30. Реагирование на нарушение режима безопасности, процедуры плановых восстановительных работ.

2.6. Оценочные критерии

При оценке знаний на экзамене учитывается: правильность и осознанность изложения содержания ответа на вопросы, полнота раскрытия понятий

и закономерностей, точность употребления и трактовки общенаучных и специальных терминов; самостоятельность ответа; речевая грамотность и логическая последовательность ответа.

Критерии оценок:

- отлично – полно раскрыто содержание вопросов в объеме программы и рекомендованной литературы; четко и правильно даны определения и раскрыто содержание концептуальных понятий, закономерностей, корректно использованы научные термины; для доказательства использованы различные теоретические знания, выводы из наблюдений и опытов; ответ самостоятельный, исчерпывающий, без наводящих дополнительных вопросов, с опорой на знания, приобретенные в процессе специализации по выбранному направлению информатики.
- хорошо – раскрыто основное содержание вопросов; в основном правильно даны определения понятий и использованы научные термины; ответ самостоятельный; определения понятий неполные, допущены нарушения последовательности изложения, небольшие неточности при использовании научных терминов или в выводах и обобщениях, исправляемые по дополнительным вопросам экзаменаторов.
- удовлетворительно – усвоено основное содержание учебного материала, но изложено фрагментарно, не всегда последовательно; определение понятий недостаточно четкое; не использованы в качестве доказательства выводы из наблюдений и опытов или допущены ошибки при их изложении; допущены ошибки и неточности в использовании научной терминологии, определении понятий.
- неудовлетворительно – ответ неправильный, не раскрыто основное содержание программного материала; не даны ответы на вспомогательные вопросы экзаменаторов; допущены грубые ошибки в определении понятий, при использовании терминологии.

3. Учебно-методические материалы по дисциплине

3.1. Используемая и рекомендуемая литература

Основная:

1. Бармен С. Разработка правил информационной безопасности.: Пер. с англ. - М.: Издательский дом «Вильямс», 2002. - 208 с.
2. Петренко С. А., Петренко А. А. Аудит безопасности Intranet. - М.: ДМК Пресс, 2002. - 416 с. (Информационные технологии для инженеров).
3. Столлингс В. Криптография и защита сетей: принципы и практика. Пер. с англ. - М.: Изд. дом «Вильямс», 2001. - 672 с.
4. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Издательство ТРИУМФ, 2002 - 816 с.: ил.

Дополнительная:

1. Герасименко В.А., Скворцов А.А., Харитонов И.Е. Новые направления

применения криптографических методов защиты информации.- М.: Радио и связь, 1989. – 360 с.
2. Диффи У. Первые 10 лет криптографии с открытым ключом // ТИИЭР, 1988, т. 76, N 5, с. 54-74 Методы, система RSA.
3. Защита программного обеспечения / Д. Гроувер – М.: Мир, 1992. – 280 с.
4. Петраков А.В. Защита и охрана личности, собственности, информации. – М.: Радио и связь, 1997. – 320 с.
5. Месси Дж.Л. Введение в современную криптологию // ТИИЭР, 1988, т. 76, N 5, с. 24-42.
6. Спесивцев А.В. Защита информации в персональных ЭВМ. – М.: Радио и связь, 1992. – 190 с.
7. Хоффман Л.Д. Современные методы защиты информации / Под ред. В.А. Герасименко. – М.: Сов. радио, 1980. – 264 с.
8. Баричев С. В. Криптография без секретов. – М.: Наука, 1998. – 120 с.
9. Кузьмин И.Н. Защита информации и информационная безопасность. Учебно-методическое пособие -Благовещенск: АмГУ, 2002. - 49 с.

4. Учебно-методическая (технологическая) карта дисциплины

Номер недели	Номер темы	изучаемые на лекцииВопросы,	Занятия		Используемые наглядные и методические пособия	Самостоятельная работа студентов		Форма контроля
			Практические	Лабораторные		*Содержание*	*Часы*	
1	2	3	4	5	6	7	8	9

1	1	1-3	-	1	1	Поиск литературы по самостоятельной работы	10	злр
2	2			2	2			злр
3		4-6		3	3			злр
4	3				3	Работа с литературой и поиск информации в сети Интернет	22	злр
5								злр, сб.
6	4	5-3		4	2			
7		7-10		5	4	Написание отчета	12	злр
8	5							злр, защ.
9	6			6				
10					2			
11		6-9						
12	7				1	Защита отчета по самостоятельной работе	10	злр
13				7	2			злр, защ.
14								
15	8	10-12						

Условные обозначения:
Осн.- основная литература
Доп. Дополнительная литература
К.р. – контрольная работа
Сб. – собеседование
Злр – защита лабораторной работы

Приложение А

Образец тестовых заданий

Вариант 1

1. **Меры информационной безопасности направлены на защиту от**:
   - нанесения неприемлемого ущерба
   - нанесения любого ущерба
   - подглядывания в замочную скважину

2. Что из перечисленного не относится к числу основных аспектов информационной безопасности?

- доступность
- целостность
- конфиденциальность
- правдивое отражение действительности

3. Затраты организаций на информационную безопасность:

- растут
- остаются на одном уровне

- снижаются

4. Что такое защита информации?

- защита от несанкционированного доступа к информации
- выпуск бронированных коробочек для дискет
- комплекс мероприятий, направленных на обеспечение информационной безопасности

5. Компьютерная преступность в мире:

- остается на одном уровне
- снижается
- растет

2. ГРАФИК САМОСТОЯТЕЛЬНОЙ УЧЕБНОЙ РАБОТЫ СТУДЕНТОВ

Понятие «самостоятельная работа» имеет две стороны: во-первых, это единственный метод усвоения знаний, во-вторых, это одна из организационных форм обучения.

Самостоятельная работа студентов включает следующие виды работ:

- подготовку к семинарам, практическим занятиям, зачету, экзамену;
- работу с периодическими изданиями, с нормативно-правовой документацией;
- подготовка отчета по лабораторным занятиям.

Распределение часов и заданий самостоятельной работы студентов по темам:

Тема 1. Экранирование, анализ защищенности (10 часов)

Контрольные вопросы:

1. Какие функции выполняет экран?
2. Что обеспечивает экранирование на сетевом уровне?
3. Где располагается демилитаризованная зона?
4. Какие принципы архитектурной безопасности применяются к сетевым экранам?
5. Что обеспечивает комплексное экранирование?

Тема 2. Обеспечение высокой доступности (12 часов)

Контрольные вопросы:

1. Когда информационный сервис считается недопустимым?
2. От чего зависит среднее время наработки на отказ?
3. Чем измеряется эффективность информационного сервиса?
4. Как можно найти интенсивности отказов независимых компонентов?
5. Основные угрозы доступности.

Тема 3. Туннелирование и управление (10 часов)

Контрольные вопросы:

1. В чем сущность каркаса?
2. Архитектурные элементы системы управления.
3. Возможности типичных систем.
4. Система активного аудита.
5. Стандарт X.700.

Тема 4. Распространение объектно-ориентированного подхода на ИБ (10 часов)

Контрольные вопросы:

1. О необходимости объектно-ориентированного подхода к ИБ
2. Основные понятия объектно-ориентированного подхода
3. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем
4. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения.
5. На что опирается структурный подход?

Тема 5. Защита информации от утечки по техническим каналам (12 часов)

Контрольные вопросы:

1. Каналы утечки информации.
2. Защита информации от утечки по визуально-оптическим каналам.
3. Защита информации от утечки по акустическим каналам.
4. Защита информации от утечки по электромагнитным каналам.
5. Защита информации от утечки по материально-вещественным каналам.

3. КОНСПЕКТ ЛЕКЦИЙ ПО ДИСЦИПЛИНЕ

Тема 1. АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ ОБРАБОТКИ ДАННЫХ КАК ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

Предмет и объекты защиты информации

Применение различных информационных технологий в организационном управлении происходит в основном посредством разработки и внедрения соответствующих их автоматизированных систем обработки информации (АСОИ). АСОИ является ядром автоматизированной системы организационного управления (АСОУ), предназначенной для комплексной автоматизации всех или большинства основных функций органов управления: сбор и анализ информации, планирование и принятие решений, доведение решений до исполнителей и контроль исполнения и т. д.

При создании современных АСОИ приходится решать две достаточно противоречивые задачи: минимальная стоимость и обеспечение безопасности компьютерных систем.

Представим (рис. 1) АСОУ в виде совокупности объекта (или объектов) управления (например, различных предприятий) и субъекта управления (управленческого аппарата). Управленческий аппарат формирует цели, разрабатывает планы, принимает определенные управленческие решения и весь этот поток информации по прямой связи направляется к объекту (или объектам) управления. Задачами объекта управления являются выполнение планов

(реализация поставленных целей. Для целенаправленной деятельности управленческого аппарата по обратной связи в субъект управления передается информация о текущем состоянии объекта управления (отчетная информация).

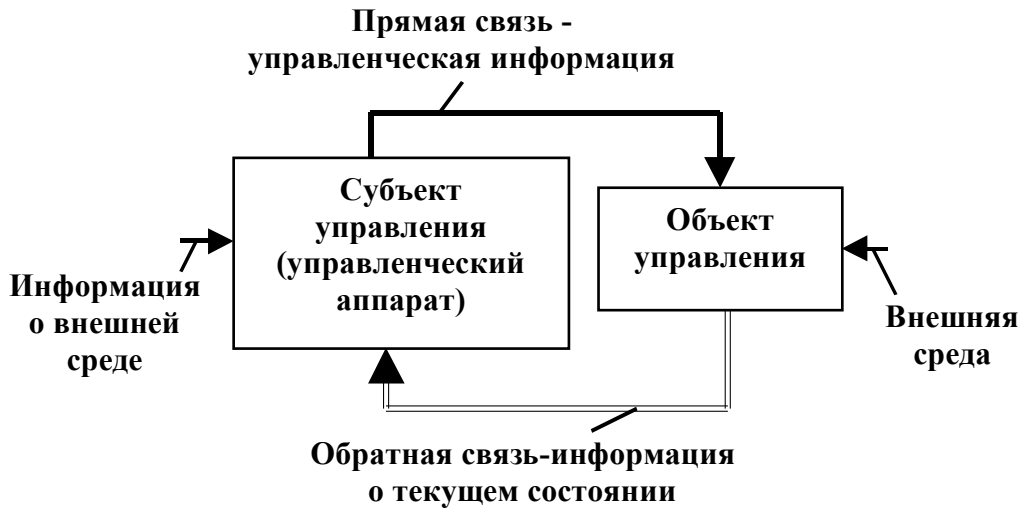


Рис. 1. Структура системы управления

Таким образом целенаправленное и успешное функционирование всей системы управления в основном зависит от качественного и эффективного функционирования информационной системы. Следовательно ИНФОРМАЦИЯ ЯВЛЯЕТСЯ ПРЕДМЕТОМ ЗАЩИТЫ (ресурсы также защищаются, но только в необходимых случаях).

Сложность современных автоматизированных систем управления, использование автоматизированного ввода, хранения, обработки, передачи и вывода информации делают проблему защиты еще более значительным. Этому способствовали: увеличение объемов обрабатываемой, накапливаемой, хранимой, передаваемой и выводимой информации; сосредоточение в интегральных базах данных информации различного назначения и принадлежности; расширение круга пользователей, имеющих доступ к ресурсам вычислительной системы и находящимся в ней массивам данных; широкое внедрение многопрограммного режима, режимов разделение времени и реального времени; использование персональных ЭВМ, расширяющих возможности не только пользователей, но и нарушителей.

Коротко отметим некоторые наиболее важные свойства информации и основные термины и определения.

Информация (в программировании) – это сведения, неизвестные до ее получения. Сведения, которые передаются через ЭВМ другому человеку или другой машине и является предметом защиты.

Ценная информация – это та информация, обладание которой дает возможность ее владельцу (существующему или потенциальному) получить материальный, моральный, политический или иной выигрыш. Поэтому у владельца информации возникает необходимость ее защиты. Именно “ценность” является основным критерием при принятии решений о ее защите. Оценка ценности информации до сих пор остается весьма субъективным. Часто используется также критерий “важность информации” (незаменимая жизненно

важная информация, важная информация, полезная информация, несущественная информация). Категория важности, как и ценность информации, обычно изменяется со временем и зависит от степени отношения к ней различных групп потребителей и потенциальных нарушителей.

Уровень секретности – это административная или законодательная мера, соответствующая мере ответственности лица за потерю или утечку конкретной секретной информации, регламентируемой специальным документом, с учетом определенных служебных или частных интересов. Подвергнутая несанкционированным изменениям несекретная информация может привести к потере (или утечке) связанной с ней секретной информации, а иногда и к невыполнению системой заданных функций (из-за не обнаружения пользователем нужных данных).

В настоящее время под безопасностью информации в АСОИ понимается не только опасность ее несанкционированного получения во все время нахождения в АСОИ, но и как безопасность действий, для осуществления которых используется эта информация

Безопасность информации – защита информации от утечки, модификации и утраты.

Безопасность АСОИ – защита систем обработки данных от внешних несанкционированных преднамеренных и случайных воздействий.

Достоверность информации – метод обработки информации, обеспечивающий с заданной точностью возможность контроля ее целостности при обработке, хранении и передаче по каналам и линиям связи.

Аутентификация – проверка подлинности субъекта или объекта.

Абонентское шифрование – шифрование информации в вычислительных сетях или АСУ от пользователя к пользователю.

Законодательные меры по защите информации – меры предупреждения нарушителя, определяющие меру его ответственности за совершение несанкционированных действий, оговоренных законом, по отношению к информации, подлежащей защите.

Защита информации от несанкционированного доступа (НСД) – средства, обеспечивающие безопасность информации.

Криптография – метод специального преобразования информации с целью ее сокрытия от посторонних лиц.

Кодирование информации – преобразование информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и ввода-вывода.

Модификация информации – несанкционированное изменение информации, корректное по форме и содержанию, но другое по смыслу.

Несанкционированный доступ (НСД) к информации – несанкционированные действия нарушителя, выразившиеся в разрушении, хищении, модификации информации или ознакомлении с ее содержанием.

Объект защиты информации – система обработки данных, содержащая информацию, подлежащую защите.

Предмет защиты в АСОИ – информация, подлежащая защите, указанная в техническом задании на АСОИ.

Пароль – строка или последовательность символов, недоступных для посторонних и предназначенных для идентификации и аутентификации субъектов или объектов между собой.

Прочность защиты – вероятность непреодаления защиты нарушителем за определенный промежуток времени.

Программный вирус – специально разработанная программа-вредитель, имеющая способность разрушать и видоизменять программное обеспечение АСОИ и воспроизводить себе подобных.

Система защиты информации в АСОИ – система, встроенная в структуру АСОИ, представляющая собой регулируемый целостный механизм, состоящий из системы взаимосвязанных централизованно управляемых преград, перекрывающих каналы несанкционированного доступа к информации, подлежащей защите.

В АСОИ информация имеет свой жизненный цикл. Полученная информация в начале оценивается на достоверность и полезность. Остальные этапы жизненного цикла информации иллюстрируются на рис.2. На каждом этапе жизненного цикла информация, с точки зрения ее защиты, оценивается поразному.

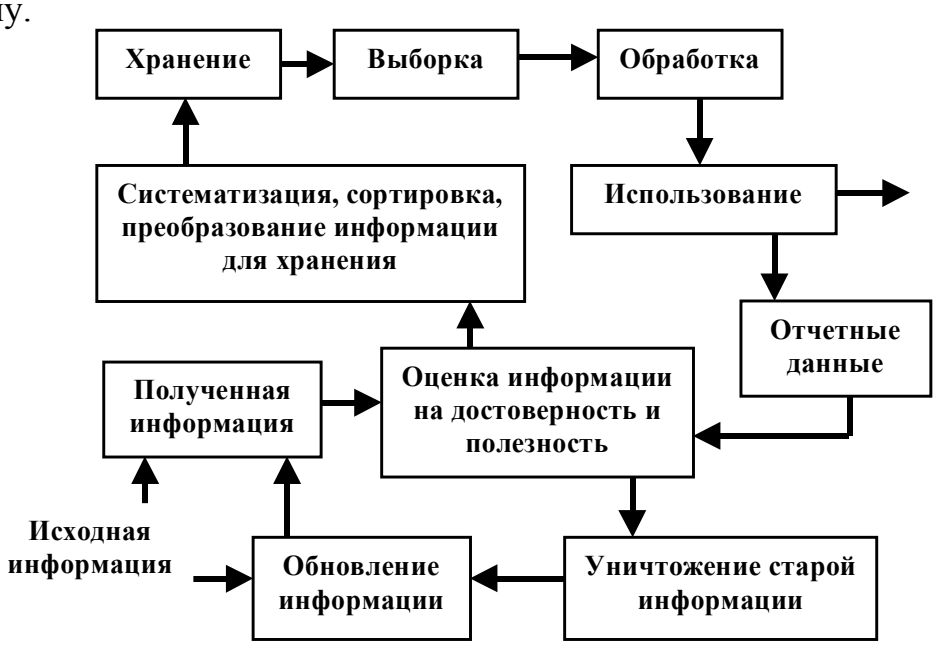


Рис. 2. Жизненный цикл информации в АСОД

При выборе и разработке методов защиты информации и их внедрении существенную роль играют формы ее машинного представления, используемые способы физического представления, структуры данных, используемые физические носители сообщений и т. д.

По существу сфера безопасности информации – не защита информации, а защита прав собственности на нее. Информация, хотя и имеет ряд существенных особенностей, наряду с традиционными материальными объектами может и должна рассматриваться законом как объект права соб-

ственности – Первая часть Гражданского кодекса РФ (ст. 128), принятый Государственной Думой (21.10.94 г.).

Особенности информации как объекта права собственности:

1) информация не материальный объект (Информация не являясь материальным объектом неразрывно связана с материальным носителем (мозг человека, книга, дискета и т.д.));

2) информация как объект права собственности легко перемещается к другому субъекту права собственности (Материальный объект права собственности не копируем (две одинаковые вещи состоят из одинаковых структур, но материально разных молекул). Информация при копировании не изменяется (те же знания, та же семантика));

3) Информация, как правило, отчуждаема от собственника (хранится и обрабатывается в сфере доступности большого числа субъектов, не являющихся субъектами права собственности на эту информацию. Перемещение материального объекта к другому субъекту влечет за собой очевидную утрату этого объекта первоначальным субъектом права собственности (нарушение прав собственности)

Физическое представление информации.

Физическое представление информации, а также процессы ее обработки говорят о том, что защита информации должна быть направлена также на защиту содержащих эту информации аппаратных и программных средств ИС.

АСОИУ представляет собой сложные комплексы коллективов специалистов, автоматизированных и иных технических средств, математического, программного, информационного, лингвистического и правового обеспечения, предназначенные для сбора, переработки, хранения и передачи (выдачи) информации. Общая структура таких АСОИУ обычно соответствует иерархической структуре органов управления и принятым в них процессам управления.

Перечислим потенциальные каналы несанкционированного (НСД) доступа к информации для типового объекта автоматизированной обработки информации с централизованной обработкой данных:

1. НСД к терминалам и ПЭВМ;
2. НСД к средствам отображения информации;
3. НСД к носителям информации;
4. НСД к средствам загрузки программного обеспечения;
5. НСД к информации при ремонте и профилактике аппаратуры;
6. НСД к внутреннему монтажу аппаратуры;
7. НСД к линиям связи;
8. НСД к каналам связи;
9. НСД к информации за счет побочного электромагнитного излучения информации;
10. НСД к информации за счет наводок на цепях электропитания и заземления;

11. НСД к информации за счет наводок на цепях вспомогательной и посторонней аппаратуры;
12. НСД к технологическим пультам;
13. Доступ к отходам носителей информации.

В результате вышеизложенного можно следующим образом ответить на вопрос – ЧТО ТАКОЕ БЕЗОПАСНОСТЬ АСОИУ ?

Под безопасностью АСОИУ понимается такое ее свойство, которое выражается в способности противодействовать попыткам нанесения ущерба владельцам и пользователям системы при различных возмущающих (умышленных−преднамеренных и неумышленных−случайных) воздействиях на нее. Природа воздействия может быть самой различной. Безопасность АСОИУ достигается:

1) обеспечением конфиденциальности обрабатываемой информации (информация должна быть известна только допущенным и прошедшим проверку субъектам системы (пользователям, программам, процессам и т. д.);

2) целостностью компонентов (ресурсов) системы (свойство компонента быть в семантическом смысле неизменным при функционировании системы);

3) доступностью компонентов и ресурсов системы (свойство компонента быть доступным для использования автоматизированными субъектами системы в любое время).

Тема 2. ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ.

Информация может существовать в различных формах в виде совокупностей некоторых знаков (символов, сигналов и т.п.) на носителях различных типов. В связи с бурным процессом информатизации общества все большие объемы информации накапливаются, хранятся и обрабатываются в автоматизированных системах, построенных на основе современных средств вычислительной техники и связи. В данной работе будут рассматриваться только те формы представления информации, которые используются при ее автоматизированной обработке.

В дальнейшем субъектами будем называть государство (в целом или отдельные его органы и организации), общественные или коммерческие организации (объединения) и предприятия (юридических лиц), отдельных граждан (физических лиц).

В процессе своей деятельности субъекты могут находиться друг с другом в разного рода отношениях, в том числе, касающихся вопросов получения, хранения, обработки, распространения и использования определенной информации. Такие отношения между субъектами будем называть *информационными отношениями*, а самих участвующих в них субъектов - *субъектами информационных отношений*.

Под автоматизированной системой обработки информации (АС) будем понимать организационно-техническую систему, представляющую собой совокупность следующих взаимосвязанных компонентов:

- технических средств обработки и передачи данных (средств вычислительной техники и связи);
- методов и алгоритмов обработки в виде соответствующего программного обеспечения;
- информации (массивов, наборов, баз данных) на различных носителях;
- персонала и пользователей системы, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации (данных) с целью удовлетворения информационных потребностей субъектов информационных отношений.

Под обработкой информации в АС будем понимать любую совокупность операций (прием, сбор, накопление, хранение, преобразование, отображение, выдача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием средств АС.

Различные субъекты по отношению к определенной информации могут выступать в качестве (возможно одновременно):

- источников (поставщиков) информации;
- пользователей (потребителей) информации;
- собственников (владельцев, распорядителей) информации;
- физических и юридических лиц, о которых собирается информация;
- владельцев систем сбора и обработки информации и участников процессов обработки и передачи информации и т.д.

Для успешного осуществления своей деятельности по управлению объектами некоторой предметной области субъекты информационных отношений могут быть заинтересованы в обеспечении:

- своевременного доступа (за приемлемое для них время) к необходимой им информации;
- конфиденциальности (сохранения в тайне) определенной части информации;
- достоверности (полноты, точности, адекватности, целостности) информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации (то есть от дезинформации);
- защиты части информации от незаконного ее тиражирования (защиты авторских прав, прав собственника информации и т.п.);
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации.

Будучи заинтересованным в обеспечении хотя бы одного из вышена-

званных требований субъект информационных отношений является уязвимым, то есть потенциально подверженным нанесению ему ущерба (прямого или косвенного, материального или морального) посредством воздействия на критичную для него информацию и ее носители либо посредством неправомерного использования такой информации. Поэтому все субъекты информационных отношений заинтересованы в обеспечении своей информационной безопасности (конечно в различной степени в зависимости от величины ущерба, который им может быть нанесен).

Для удовлетворения законных прав и перечисленных выше интересов субъектов (обеспечения их информационной безопасности) необходимо постоянно поддерживать следующие свойства информации и систем ее обработки:

- ***доступность информации***, то есть свойство системы (среды, средств и технологии ее обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость;
- ***целостность информации***, то есть свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). Точнее говоря, субъектов интересует обеспечение более широкого свойства - достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, то есть ее неискаженности. Однако, мы ограничимся только рассмотрением вопросов обеспечения целостности информации, так как вопросы обеспечения адекватности отображения выходят далеко за рамки проблемы обеспечения информационной безопасности;
- ***конфиденциальность информации*** - субъективно определяемую (приписываемую) характеристику (свойство) информации, указывающую на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемую способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты законных интересов других субъектов информационных отношений.

Поскольку ущерб субъектам информационных отношений может быть нанесен опосредовано, через определенную информацию и ее носители (в том числе автоматизированные системы обработки), то закономерно возникает заинтересованность субъектов в обеспечении безопасности этой информации и систем ее обработки и передачи. Иными словами, в качестве объектов, подлежащих защите в интересах обеспечения безопасности субъектов

информационных отношений, должны рассматриваться: информация, ее носители и процессы ее обработки.

Однако, всегда следует помнить, что уязвимыми в конечном счете являются именно заинтересованные в обеспечении определенных свойств информации и систем ее обработки субъекты (информация, равно как и средства ее обработки, не имеет своих интересов, которые можно было бы ущемить и нанести тем самым ущерб). В дальнейшем, говоря об обеспечении безопасности АС или циркулирующей в системе информации, всегда будем понимать под этим косвенное обеспечение безопасности субъектов, участвующих в процессах автоматизированного информационного взаимодействия.

В свете сказанного, термин "безопасность информации" нужно понимать как *защищенность* информации от нежелательного для соответствующих субъектов информационных отношений ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Поскольку субъектам информационных отношений ущерб может быть нанесен также посредством воздействия на процессы и средства обработки критичной для них информации, то становится очевидной необходимость обеспечения защиты всей системы обработки и передачи данной информации от несанкционированного вмешательства в процесс ее функционирования, а также от попыток хищения, незаконной модификации и/или разрушения любых компонентов данной системы.

Поэтому под безопасностью автоматизированной системы обработки информации (компьютерной системы) будем понимать защищенность всех ее компонентов (технических средств, программного обеспечения, данных и персонала) от подобного рода нежелательных для соответствующих субъектов информационных отношений воздействий.

Безопасность любого компонента (ресурса) АС складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

Конфиденциальность компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

Целостность компонента системы предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени.

Доступность компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

В свете приведенного выше подчеркнем, что конечной целью защиты АС и циркулирующей в ней информации является предотвращение или минимизация наносимого субъектам информационных отношений ущерба (прямого или косвенного, материального, морального или иного) посредством нежелательного воздействия на компоненты АС, а также разглашения (утечки),

искажения (модификации), утраты (снижения степени доступности) или незаконного тиражирования информации.

Наибольшую сложность при решении вопросов обеспечения безопасности конкретных информационно-управляющих систем (информационных технологий) представляет задача определения реальных требований к уровням защиты критичной для субъектов информации, циркулирующей в АС. Ориентация на интересы субъектов информационных отношений дает ключ к решению данной задачи для общего случая.

Исторически сложившийся подход к классификации государственной информации (данных) по уровням требований к ее защищенности основан на рассмотрении и обеспечении только одного свойства информации - ее конфиденциальности (секретности). Требования же к обеспечению целостности и доступности информации, как правило, лишь косвенно фигурируют среди общих требований к системам обработки этих данных. Считается, что раз к информации имеет доступ только узкий круг доверенных лиц, то вероятность ее искажения (несанкционированного уничтожения) незначительна. Низкий уровень доверия к АС и предпочтение к бумажной информационной технологии еще больше усугубляют ограниченность данного подхода.

Если такой подход в какой-то степени оправдан в силу существующей приоритетности свойств безопасности важной государственной информации, то это вовсе не означает, что его механический перенос в другую предметную область (с другими субъектами и их интересами) будет иметь успех.

Во многих областях деятельности (предметных областях) доля конфиденциальной информации сравнительно мала. Для коммерческой и персональной информации, равно как и для государственной информации, не подлежащей засекречиванию, приоритетность свойств безопасности информации может быть иной. Для открытой информации, ущерб от разглашения которой несущественен, важнейшими могут быть такие качества, как доступность, целостность или защищенность от неправомерного тиражирования. К примеру, для платежных (финансовых) документов самым важным является свойство их целостности (достоверности, неискаженности). Затем, по степени важности, следует свойство доступности (потеря платежного документа или задержка платежей может обходиться очень дорого). Требований к обеспечению конфиденциальности отдельных платежных документов может не предъявляется вообще.

Попытки подойти к решению вопросов защиты такой информации с позиций традиционного обеспечения только конфиденциальности, терпят провал. Основными причинами этого, на наш взгляд, являются узость существующего подхода к защите информации, отсутствие опыта и соответствующих проработок в плане обеспечения целостности и доступности информации, не являющейся конфиденциальной.

Развитие системы классификации информации по уровням требований к ее защищенности предполагает введение ряда степеней (градаций) требований по обеспечению каждого из свойств безопасности информации: доступности, целостности, конфиденциальности и защищенности от тиражирования. Пример градаций требований к защищенности:

- нет требований;
- низкие;
- средние;
- высокие;
- очень высокие.

Количество дискретных градаций и вкладываемый в них смысл могут различаться. Главное, чтобы требования к защищенности различных свойств информации указывались отдельно и достаточно конкретно (исходя из серьезности возможного наносимого субъектам информационных отношений ущерба от нарушения каждого из свойств безопасности информации).

В дальнейшем любой отдельный функционально законченный документ (некоторую совокупность знаков), содержащий определенные сведения, вне зависимости от вида носителя, на котором он находится, будем называть ***информационным пакетом***.

К одному типу информационных пакетов будем относить пакеты (типовые документы), имеющие сходство по некоторым признакам (по структуре, технологии обработки, типу сведений и т.п.).

Задача состоит в определении реальных уровней заинтересованности (высокая, средняя, низкая, отсутствует) субъектов в обеспечении требований к защищенности каждого из свойств различных типов информационных пакетов, циркулирующих в АС.

Требования же к системе защиты АС в целом (методам и средствам защиты) должны определяться, исходя из требований к защищенности различных типов информационных пакетов, обрабатываемых в АС, и с учетом особенностей конкретных технологий их обработки и передачи (уязвимости).

В одну категорию объединяются типы информационных пакетов с равными приоритетами и уровнями требований к защищенности (степенью важности обеспечения их свойств безопасности : доступности, целостности и конфиденциальности).

Предлагаемый порядок определения требований к защищенности циркулирующей в системе информации представлен ниже:

1. Составляется общий перечень типов информационных пакетов, циркулирующих в системе (документов, таблиц). Для этого с учетом предметной области системы пакеты информации разделяются на типы по ее тематике, функциональному назначению, сходности технологии обработки и т.п. признакам.

На последующих этапах первоначальное разбиение информации (данных) на типы пакетов может уточняться с учетом требований к их защищенности.

2. Затем для каждого типа пакетов, выделенного в первом пункте, и каждого критического свойства информации (доступности, целостности, конфиденциальности) определяются (например, методом экспертных оценок):

- перечень и важность (значимость по отдельной шкале) субъектов, интересы которых затрагиваются при нарушении данного свойства информации;
- уровень наносимого им при этом ущерба (незначительный, малый, средний, большой, очень большой и т.п.)и соответствующий уровень требований к защищенности.

При определении уровня наносимого ущерба необходимо учитывать:

- стоимость возможных потерь при получении информации конкурентом;
- стоимость восстановления информации при ее утрате;
- затраты на восстановление нормального процесса функционирования АС и т.д.

Если возникают трудности из-за большого разброса оценок для различных частей информации одного типа пакетов, то следует пересмотреть деление информации на типы пакетов, вернувшись к предыдущему пункту методики.

3. Для каждого типа информационных пакетов с учетом значимости субъектов и уровней наносимого им ущерба устанавливается степень необходимой защищенности по каждому из свойств информации (при равенстве значимости субъектов выбирается максимальное значение уровня).

Пример оценки требований к защищенности некоторого типа информационных пакетов приведен в таблице 1.

Таблица 1.

Субъекты	Уровень ущерба по свойствам информации			
	Конфиденциальность	Целостность	Доступность	Защита от тиражирования
N 1	Нет	Средняя	Средняя	Нет
N 2	Высокая	Средняя	Средняя	Нет
N m	Низкая	Низкая	Низкая	Нет
В итоге	Высокая	Средняя	Средняя	Нет

К определению основных понятий в области безопасности информационных технологий и общих целей защиты надо подходить с позиции защиты интересов и законных прав субъектов информационных отношений. Необходимо всегда помнить, что защищать надо именно субъектов информационных отношений, так как в конечном счете именно им, а не самой информации или системам ее обработки может наноситься ущерб. Иными словами, защита информации и систем ее обработки - вторичная задача. Главная задача - это защита интересов субъектов информационных отношений. Такая расстановка акцентов позволяет правильно определять требования к защищенности конкретной информации и систем ее обработки.

В соответствии с возможной заинтересованностью различных субъектов информационных отношений существует четыре основных способа нанесе-

ния им ущерба посредством разного рода воздействий на информацию и системы ее обработки:

- нарушение конфиденциальности (раскрытие) информации;
- нарушение целостности информации (ее полное или частичное уничтожение, искажение, фальсификация, дезинформация);
- нарушение (частичное или полное) работоспособности системы. Вывод из строя или неправомерное изменение режимов работы компонентов системы обработки информации, их модификация или подмена могут приводить к получению неверных результатов расчетов, отказам системы от потока информации (непризнанию одной из взаимодействующих сторон факта передачи или приема сообщений) и/или отказам в обслуживании конечных пользователей;
- несанкционированное тиражирование открытой информации (не являющейся конфиденциальной), например, программ, баз данных, разного рода документации, литературных произведений и т.д. в нарушение прав собственников информации, авторских прав и т.п. Информация, обладая свойствами материальных объектов, имеет такую особенность, как неисчерпаемость ресурса, что существенно затрудняет контроль за ее тиражированием.

Защищать АС (с целью защиты интересов субъектов информационных отношений) необходимо не только от несанкционированного доступа (НСД) к хранимой и обрабатываемой в них информации, но и от неправомерного вмешательства в процесс ее функционирования, нарушения работоспособности системы, то есть от любых несанкционированных действий. Защищать необходимо все компоненты АС: оборудование, программы, данные, персонал.

Механический перенос подходов к обеспечению безопасности субъектов информационных отношений из одной предметной области в другую, как правило, успеха не имеет. Причина этого - существенные различия интересов субъектов в разных предметных областях, в частности, различия в приоритетах свойств защищаемой информации и требований к характеристикам систем обработки информации.

Требования к уровню защищенности критичных свойств информационных пакетов различных типов (документов, справок, отчетов и т.п.) в конкретной предметной области должны устанавливаться ее владельцами (собственниками) или другими субъектами информационных отношений на основе анализа серьезности последствий нарушения каждого из свойств информации (типов информационных пакетов): доступности, целостности и конфиденциальности.

Прежде чем переходить к рассмотрению основных задач и подходов к построению систем защиты, призванных обеспечить надлежащий уровень безопасности субъектов информационных отношений, надо уточнить, от какого рода нежелательных воздействий необходимо защищать информацию и автоматизированные системы ее обработки и передачи.

Как показывает анализ, большинство современных автоматизированных

систем обработки информации в общем случае представляет собой территориально распределенные системы интенсивно взаимодействующих (синхронизирующихся) между собой по данным (ресурсам) и управлению (событиям) локальных вычислительных сетей (ЛВС) и отдельных ЭВМ.

В распределенных АС возможны все "традиционные" для локально расположенных (централизованных) вычислительных систем способы несанкционированного вмешательства в их работу и доступа к информации. Кроме того, для них характерны и новые специфические каналы проникновения в систему и несанкционированного доступа к информации, наличие которых объясняется целым рядом их особенностей.

Перечислим основные из особенностей распределенных АС:

- территориальная разнесенность компонентов системы и наличие интенсивного обмена информацией между ними;
- широкий спектр используемых способов представления, хранения и передачи информации;
- интеграция данных различного назначения, принадлежащих различным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в различных удаленных узлах сети;
- абстрагирование владельцев данных от физических структур и места размещения данных;
- использование режимов распределенной обработки данных;
- участие в процессе автоматизированной обработки информации большого количества пользователей и персонала различных категорий;
- непосредственный и одновременный доступ к ресурсам (в том числе и информационным) большого числа пользователей (субъектов) различных категорий;
- высокая степень разнородности используемых средств вычислительной техники и связи, а также их программного обеспечения;
- отсутствие специальной аппаратной поддержки средств защиты в большинстве типов технических средств, широко используемых в АС.

В общем случае АС состоят из следующих основных структурно-функциональных элементов:

- рабочих станций - отдельных ЭВМ или удаленных терминалов сети, на которых реализуются автоматизированные рабочие места пользователей (абонентов, операторов);
- серверов или Host машин (служб файлов, печати, баз данных и т.п.) не выделенных (или выделенных, то есть не совмещенных с рабочими станциями) высокопроизводительных ЭВМ, предназначенных для реализации функций хранения, печати данных, обслуживания рабочих станций сети и т.п. действий;

- межсетевых мостов (шлюзов, центров коммутации пакетов, коммуникационных ЭВМ) - элементов, обеспечивающих соединение нескольких сетей передачи данных, либо нескольких сегментов одной и той же сети, имеющих различные протоколы взаимодействия;
- каналов связи (локальных, телефонных, с узлами коммутации и т.д.).

Рабочие станции являются наиболее доступными компонентами сетей и именно с них могут быть предприняты наиболее многочисленные попытки совершения несанкционированных действий. С рабочих станций осуществляется управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На видеомониторы и печатающие устройства рабочих станций выводится информация при работе пользователей (операторов), выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы. Именно поэтому рабочие станции должны быть надежно защищены от доступа посторонних лиц и содержать средства разграничения доступа к ресурсам со стороны законных пользователей, имеющих разные полномочия. Кроме того, средства защиты должны предотвращать нарушения нормальной настройки рабочих станций и режимов их функционирования, вызванные неумышленным вмешательством неопытных (невнимательных) пользователей.

В особой защите нуждаются такие привлекательные для злоумышленников элементы сетей как серверы (Host - машины) и мосты. Первые - как концентраторы больших объемов информации, вторые - как элементы, в которых осуществляется преобразование (возможно через открытую, нешифрованную форму представления) данных при согласовании протоколов обмена в различных участках сети.

Благоприятным для повышения безопасности серверов и мостов обстоятельством является, как правило, наличие возможностей по их надежной защите физическими средствами и организационными мерами в силу их выделенности, позволяющей сократить до минимума число лиц из персонала сети, имеющих непосредственный доступ к ним. Иными словами, непосредственные случайные воздействия персонала и преднамеренные воздействия злоумышленников на выделенные серверы и мосты можно считать маловероятными. В то же время, надо ожидать массированной атаки на серверы и мосты с использованием средств удаленного доступа. Здесь злоумышленники прежде всего могут искать возможности повлиять на работу различных подсистем серверов и мостов, используя недостатки протоколов обмена и средств разграничения удаленного доступа к ресурсам и системным таблицам. Использоваться могут все возможности и средства, от стандартных (без модификации компонентов) до подключения специальных аппаратных средств (каналы, как правило, слабо защищены от подключения) и применения высококлассных программ для преодоления системы защиты.

Конечно, сказанное выше не означает, что не будет попыток внедрения аппаратных и программных закладок в сами мосты и серверы, открывающих дополнительные широкие возможности по несанкционированному удаленно-

му доступу. Закладки могут быть внедрены как с удаленных станций (посредством вирусов или иным способом), так и непосредственно в аппаратуру и программы серверов при их ремонте, обслуживании, модернизации, переходе на новые версии программного обеспечения, смене оборудования.

Каналы и средства связи также нуждаются в защите. В силу большой пространственной протяженности линий связи (через неконтролируемую или слабо контролируемую территорию) практически всегда существует возможность подключения к ним, либо вмешательства в процесс передачи данных. Возможные при этом угрозы подробно изложены ниже.

Тема 3. ЗАКОНОДАТЕЛЬНЫЕ И ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В деле обеспечения информационной безопасности успех может нести только комплексный подход. Мы уже указывали, что для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного;
- административного (приказы и. другие действия руководства организаций
- процедурного (меры безопасности, ориентированные на людей);
- программно-технического.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Самое важное (и, вероятно, самое трудное) на законодательном уровне - создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

Обзор российского законодательства в области информационной безопасности

Основным законом Российской Федерации является Конституция принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 - право на знание достоверной информации о состоянии окружающей среды.

В принципе, право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удоб-

ным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

Статья 23 Конституции гарантирует право на личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 — право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам зашиты информации.

В Гражданском кодексе Российской Федерации (в своем изложении мы опираемся на редакцию от 15 мая 2001 года) фигурируют такие понятия, как банковская, коммерческая и служебная тайна.

Весьма продвинутым в плане информационной безопасности является Уголовный кодекс Российской Федерации (редакция от 14 марта 2002 года). Глава 28 — "Преступления в сфере компьютерной информации" — содержит три статьи:

- статья 272. Неправомерный доступ к компьютерной информации;
- статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Первая имеет дело с посягательствами на конфиденциальность, вторая - с вредоносным ПО, третья - с нарушениями доступности и целостности, повлекшими за собой уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ.

Статья 138 УК РФ, защищая конфиденциальность персональных данных, предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений. Аналогичную роль для банковской и коммерческой тайны играет статья 183 УК РФ.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе "О государственной тайне" (с изменениями и дополнениями от 6 октября 1997 года). В нем гостайна определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение средств защиты информации. Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Закон "Об информации, информатизации и защите информации"

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информатизации и защите информации" от 20 февраля 1995 года номер 24-ФЗ (принят Государственной Думой 25 января 1995 года). В нем даются основные определения и намечаются направления развития законодательства в данной области.

Процитируем некоторые из этих определений:

• **информация** — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

• **документированная информация (документ) —** зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

• **информационные процессы** — процессы сбора, обработки, накопления, хранения, поиска и распространения информации;

• **информационная система** - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств ни числительной техники и связи, реализующих информационные процессы;

• **информационные ресурсы** — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

• **информация о гражданах (персональные данные) —** сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

• **конфиденциальная информация** - документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации;

• **пользователь (потребитель) информации -** субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Закон выделяет следующие цели защиты информации:

• предотвращение утечки, хищения, утраты, искажения, подделки информации;

• предотвращение угроз безопасности личности, общества, государства;

• предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

• предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

• защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

•сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

• обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Отметим, что Закон на первое место ставит сохранение конфиденциальности информации. Целостность представлена также достаточно хорошо, хотя и на втором месте. О доступности ("предотвращение несанкционированных действий по ... блокированию информации") сказано довольно мало.

Продолжим цитирование:

"Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу".

По сути, это положение констатирует, что защита информации направлена на обеспечение интересов субъектов информационных отношений.

Далее. "Режим защиты информации устанавливается:

• в отношении сведений, отнесенных к государственной тайне, — уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";

• в отношении конфиденциальной документированной информации - собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;

• в отношении персональных данных — федеральным законом."

Здесь выделены три вида защищаемой информации, ко второму из которых принадлежит, в частности, коммерческая информация. Поскольку защите подлежит только документированная информация, необходимым условием является фиксация коммерческой информации на материальном носителе и снабжение ее реквизитами. Отметим, что в данном месте Закона речь идет только о конфиденциальности; остальные аспекты ИБ забыты.

Обратим внимание, что защиту государственной тайны и персональных данных берет на себя государство; за другую конфиденциальную информацию отвечают ее собственники.

Как же защищать информацию? В качестве основного закон предлагает для этой цели мощные универсальные средства: лицензирование и сертификацию. Процитируем статью 19.

1. Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации "О сертификации продукции и услуг".

2. Информационные системы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации, других государственных органов, организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации. Порядок сертификации определяется законодательством Российской Федерации организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают ли-

цензии на этот вид деятельности. Порядок лицензирования определяется законодательством Российской Федерации.

4. Интересы потребителя информации при использовании импортной продукции в информационных системах защищаются таможенными органами Российской Федерации на основе международной системы сертификации.

Здесь трудно удержаться от риторического вопроса: а есть ли в России информационные системы без импортной продукции? Получается, что на защите интересов потребителей стоит в данном случае только таможня... И еще несколько пунктов, теперь из статьи *22:*

2. Владелиц документов, массива документов, информационных систем обеспечивает уровень зашиты информации в соответствии с законодательством Российской Федерации.

3. Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих сгнетем и средств. *Риск,* связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации;

4. Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа/достаточности мер защиты его ресурсов и систем и получения консультаций.

5. Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации.

Очень важными являются пункты статьи 5, касающиеся юридической силы электронного документа и электронной цифровой подписи, юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.

Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования. Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии. Порядок выдачи лицензий определяется законодательством Российской Федерации.

Другие законы и нормативные акты

Следуя логике Закона "Об информации, информатизации и защите информации", мы продолжим наш обзор Законом о лицензировании отдельных видов деятельности (8 августа 2001). Начнем с основных определений.

"Лицензия - специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому липу или индивидуальному предпринимателю.

Лицензирующие органы — федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с настоящим Федеральным

Лицензиат— юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности."

Статья 17 Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. Нас будут интересовать следующие виды:

• распространение шифровальных (криптографических) средств;

• техническое обслуживание шифровальных (криптографических) средств:

• предоставление услуг в области шифрования информации;

• разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

• выдача сертификатов ключей электронных цифровых подписей, регистрация владельцев электронных цифровых подписей, оказание услуг, связанных с использованием электронных цифровых подписей и подтверждением подлинности электронных цифровых подписей;

• выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

• разработка и (или) производство средств зашиты конфиденциальной информации;

• техническая защита конфиденциальной информации;

• разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Необходимо учитывать, что, согласно статье 1, действие данного Закона не распространяется на следующие виды деятельности:

- деятельность, связанная с защитой государственной тайны:
- деятельность в области связи;
- образовательная деятельность.

Основными лицензирующими органами в области защиты информации являются Федеральное агентство правительственной связи и информации и Гостехкомиссия России. ФАПСИ ведает всем, что связано с криптографией, Гостехкомиссия лицензирует деятельность по защите конфиденциальной информации. Ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней может осуществляться исключительно на основании лицензии Министерства внешних экономических связей РФ, выдаваемой на основании решения ФАПСИ.

В эпоху глобальных коммуникаций важную роль играет 'Закон "Об участии в международном информационном обмене" от 4 июля 1996 года. В нем, как и в Законе "Об информации...", основным защитным средством являются лицензии и сертификаты. Процитируем несколько пунктов из статьи 9.

2. Зашита конфиденциальной информации государством распространяется только на ту деятельность по международному информационному обмену, которую осуществляют физические и юридические лица, обладающие лицеи на работу с конфиденциальной информацией и использующие сертифицированные средства международного информационного обмена.

   Выдача сертификатов и лицензий возлагается на Комитет при Президенте РФ по политике информатизации, Государственную техническую комиссию при Президенте РФ, Федеральное агентство правительственной связи и информации при Президенте Р Ф. Порядок выдачи сертификатов и лицензий устанавливается Правительством РФ.

3. При обнаружении нештатных режимов функционирования средств международного информационного обмена, то есть возникновении ошибочных команд, а также команд, вызванных несанкционированными действиями обслуживающего персонала или иных лиц, либо ложной информацией собственник или владелец этих средств должен своевременно сообщит об этом в органы контроля за осуществлением международного информационного обмена и собственник или владельцу взаимодействующих средств международного информационного обмена, в противном случае он несет ответственность за причиненный ущерб.

При желании здесь можно усмотреть обязательность выявления нарушителя информационной безопасности — положение, вне всяких сомнений, очень важное и прогрессивное.

Еще одна цитата - теперь из статьи I 7 того же Закона.

Статья 17: "Сертификация информационных продуктов, информационных услуг, средств международного информационного обмена.

1. При ввозе информационных продуктов, информационных услуг в РФ импортер представляет сертификат, гарантирующий соответствие данных продуктов и услуг требованиям договора. В случае невозможности сертификации ввозимых на территорию РФ информационных продуктов, информационных услуг ответственность за использование данных продуктов и услуг лежит на импортере.

2. Средства международного информационного обмена, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих средств подлежат обязательной сертификации.

3 Сертификация сетей связи производится в порядке, определяемом Федеральным - законом "О связи".

Читая пункт 2, трудно удержаться от вопроса; "А нужно ли сертифицировать средства защиты средств защиты от этих средств?" Ответ, конечно, положительный...

Обзор зарубежного законодательства в области информационной безопасности

Мы лишь пунктиром очертим некоторые законы нескольких стран (в первую очередь — США), поскольку только в США таких законодательных актов около 500.

Ключевую роль играет американский "Закон об информационной безопасности" (1988). Его цель - реализация минимально достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений всего спектра возможных действии.

Характерно, что уже вначале Закона называется конкретный исполнитель — Национальный институт стандартов и технологий (НИСТ), отвечающий за выпуск стандартов и руководств, направленных на защиту от уничтожения и несанкционированного доступа к информации, а так же от краж и подлогов, выполняемых с помощью компьютеров. Таким образом, имеется в виду, как регламентация действий специалистов, так и повышение информированности всего общества.

Согласно Закону, все операторы федеральных ИС, содержащих конфиденциальную информацию, должны сформировать планы обеспечения ИБ. Обязательным является и периодическое обучение всего персонала таких ИС. НИ СТ, в свою очередь, обязан проводить исследовании природы и масштаба уязвимых мест, вырабатывать экономически оправданные меры защиты. Результаты исследований рассчитаны на применение не только в государственных системах, но и в частном секторе.

Закон обязывает НИСТ координировать свою деятельность с другими министерствами и ведомствами, включая Министерство обороны, Министерство энергетики, Агентство национальной безопасности (АНБ) и т.д., чтобы избежать дублирования и несовместимости.

С практической точки зрения важен раздел 6 Закона, обязывающий все правительственные ведомства сформировать план обеспечения информационной безопасности, направленный на то, чтобы компенсировать риски и предотвратить возможный ущерб от утери, неправильного использования, несанкционированного доступа или модификации информации в федеральных системах. Копии плана направляются в НИСТ и АНБ.

В 2001 году был одобрен Палатой представителей и передан в Сенат новый вариант рассмотренного законопроекта — Сотршег 5есип1у Еппапсетет Ас1 оГ2001 (Н.К. 1259 К.Р5). В этом варианте примечательно как то, что, по сравнению с предыдущей редакцией, было убрано, так и то, что добавилось.

За четыре года (1997-2001 гг.) на законодательном и других уровнях информационной безопасности США было сделано многое. Смягчены экспортные ограничения на криптосредства (в январе 2000 г.). Сформирована инфраструктура с открытыми ключами. Разработано большое число стандартов (например, новый стандарт электронной цифровой подписи -Р1Р5 186-2, январь 2000 г.). Все это позволило не заострять более внимания на криптографии как таковой, а сосредоточиться на одном из ее важнейших приложений — аутентификации, рассматривая ее по отработанной на криптосредствах методике. Очевидно, что, независимо от судьбы законопроекта, в США будет сформирована национальная инфраструктура электронной аутентификации. В дан-

ном случае законотворческая деятельность идет в ногу с прогрессом информационных технологий.

Программа безопасности, предусматривающая экономически оправданные защитные меры и синхронизированная с жизненным циклом ИС, упоминается в законодательстве США неоднократно. Согласно пункту 3534 ("Обязанности федеральных ведомств") подглавы II ("Информационная безопасность") главы 35 ("Координация федеральной информационной политики") рубрики 44 ("Общественные издания и документы"), такая программа должна включать:

- периодическую оценку рисков с рассмотрением внутренних и внешних угроз целостности, конфиденциальности и доступности систем, а также данных, ассоциированных с критически важными операциями и ресурсами;
- правила и процедуры, позволяющие, опираясь на проведенный анализ рисков, экономически оправданным образом уменьшить риски до приемлемого уровня;
- обучение персонала с целью информирования о существующих рисках и об обязанностях, выполнение которых необходимо для их (рисков) нейтрализации;
- периодическую проверку и (пере)оценку эффективности правил и процедур;
- действия при внесении существенных изменений в систему;
- процедуры выявления нарушений информационной безопасности и реагирования на них; эти процедуры должны помочь уменьшить риски, избежать крупных потерь; организовать взаимодействие с правоохранительными органами.

Конечно, в законодательстве США имеются в достаточном количестве и положения ограничительной направленности, и директивы, защищающие интересы таких ведомств, как Министерство обороны, АНБ, ФБР, ЦРУ, но мы не будем их останавливаться.

В законодательстве ФРГ выделим весьма развернутый (44 раздела) Закон о защите данных (1990). Он целиком посвящен защите персональных данных.

Как, вероятно, и во всех других законах аналогичной направленности, в данном случае устанавливается приоритет интересов национальной безопасности над сохранением тайны частной жизни. В остальном права личности защищены весьма тщательно. Например, если сотрудник фирмы обрабатывает персональные данные в интересах частных компаний, он дает подписку о неразглашении, которая действует и после перехода на другую работу.

Государственные учреждения, хранящие и обрабатывающие персональные данные, несут ответственность за нарушение тайны частной жизни, субъекта данных", как говорится в Законе. В материальном выражении ответственность ограничена верхним пределом в 250 тысяч немецких марок.

В современном мире глобальных сетей законодательная база должна быть согласована с международной практикой. В этом плане поучителен пример Аргентины. В конце марта 1996 года компетентными органами Аргентины был арестован Хулио Цезар Ардита. 21 года, житель Буэнос-Айреса, систем-

ный оператор электронной доски объявлении "Крик", известный в компьютерном подполье под псевдонимом "El Griton". Ему вменялись в вину систематические вторжения в компьютерные системы ВМС США, НАСА, многих крупнейших американских университетов, а также в компьютерные системы Бразилии. Чили. Кореи. Мексики и Тайваня. Однако, несмотря на тесное сотрудничество компетентных органон Аргентины и США, Ардита был отпущен без официального предъявления обвинений, поскольку по аргентинскому законодательству вторжение в компьютерные системы не считается преступлением. Кроме того, в силу принципа "двойной криминальности", действующего в международных правовых отношениях. Аргентина не может выдать хакера американским властям. Дело Ардита показывает, каким может быть будущее международных компьютерных вторжений при отсутствии всеобщих или хотя бы двусторонних соглашении о борьбе с компьютерной преступностью.

Как уже отмечалось, самое важное на законодательном уровне – создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Пока такого механизма нет и, увы не предвидится.

В современном мире глобальных сетей нормативно-правовая база должна быть согласована с международной практикой. Желательно привести российские стандарты в соответствие с международным уровнем информационных технологий вообще и информационной безопасности в частности. Есть целый ряд оснований для того, чтобы это сделать. Одно из них – необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами российских компаний. Второе – доминирование аппаратно-программных продуктов зарубежного производства. На законодательном уровне должен быть решен вопрос об отношении к таким изделиям. Здесь необходимо выделить два аспекта: независимость в области информационных технологий и информационную безопасность. Использование зарубежных продуктов в некоторых критически важных системах (военных), в принципе может представлять угрозу национальной безопасности (информационной), т.к. нельзя исключить вероятности встраивания закладных элементов. Проблема сертификации аппаратно-программных продуктов зарубежного производства действительно сложна, однако как показывает опыт европейских стран, решить ее можно.

Подводя итог, можно наметить следующие основные направления деятельности на законодательном уровне:

- разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;
- обеспечение баланса созидательных и ограничительных (в первую очередь преследующих цель наказать виновных) законов;
- интеграция в мировое правовое пространство;
- учет современного состояния информационных технологий.

Тема 4. ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АСОД

Обычно при постановке задачи обеспечения безопасности АСОИУ необходимо ответить на следующие вопросы:

1. От чего нужно защищать систему?
2. Что необходимо защищать в системе?
3. Посредством каких методов и средств необходимо защищать систему?

Целью применения любых мер противодействия угрозам является защита владельца и законных пользователей АСОИУ от нанесения им материального или морального ущерба в результате случайных или преднамеренных воздействий на нее.

Различают ВНЕШНЮЮ и ВНУТРЕНЮЮ безопасность.

Внешняя безопасность АСОИУ включает защиту от стихийных бедствий и от проникновение злоумышленников извне с целью хищения, получения доступа к носителям информации или вывода системы из строя.

Внутренняя безопасность АСОИ должна обеспечивать надежную и корректную работу системы, целостность ее программ и данных.

Для решения задачи защиты информации необходимо определить природу угроз, формы и пути их возможного проявления и осуществления в АСОИУ. Многочисленные случаи воздействия на информацию и несанкционированного доступа к ней можно разделить как множество угроз на СЛУЧАЙНЫЕ и ПРЕДНАМЕРЕННЫЕ воздействия.

Информация в процессе ввода, хранения, обработки, вывода и передачи подвергается различным случайным воздействиям. На аппаратном уровне это приводит к физическим изменениям уровней сигналов в цифровых кодах (изменение значения кода – для обнаружения применяются средства функционального контроля). Если отсутствуют средства обнаружения и исправления подобных сбоев, то происходит модификация информации. В результате в зависимости от содержания и назначения ложного кода дальнейший процесс обработки данных может протекать по нескольким ложным путям и привести к различным катастрофическим (или ложным) результатам (изменение команды и ее выполнение, изменение данного и получение неверного результата, на программном уровне изменения алгоритма обработки данных и т. д.). Причины случайного воздействия при эксплуатации АСОИУ могут быть следующими:

1) отказы и сбои аппаратуры;
2) схемные и системотехнические ошибки разработчиков;
3) помехи на линиях связи от воздействий внешней среды;
4) структурные, алгоритмические и программные ошибки;
5) ошибки человека как звена системы;
6) аварийные ситуации и другие воздействия.

С усложнением АСОИУ при разработке увеличиваются схемные, системотехнические, структурные, алгоритмические и программные ошибки (влияющие факторы – квалификация разработчиков, условия их работы, наличие опыта и др.

Ошибки человека могут подразделяться на:

1. Логические (неправильно принятые решения);
2. Сенсорные (неправильное восприятие информации);

3. Оперативные или моторные (неправильная реализация решения).

Интенсивность ошибок человека может колебаться в пределах от 1 – 2% до 15 – 40%. Особенно важное значение проблема борьбы с ошибками человека как звена системы приобретает в автоматизированных системах управления административного управления.

К аварийным ситуациям относятся:

- Отказ функционирования АСОИ в целом (например, выход из строя электропитания);
- Стихийные бедствия;
- Отказ системы жизнеобеспечения на объекте эксплуатации АСОИ.

Более подробно рассмотрим преднамеренные угрозы безопасности АСОИ. Реализация угрозы будет называться АТАКОЙ. Классификацию угроз безопасности будем производить по отдельным признакам (см. рис.1.9).

По цели реализации угрозы:

- Нарушение конфиденциальности информации (информация в АСОИ имеет большую ценность для ее владельца и ее использование другими лицами наносит значительный ущерб интересам владельца);
- Нарушение целостности информации (полная или частичная дезинформация – ценная информация может быть утрачена или обесценена путем ее несанкционированного удаления или модификации). Ущерб может быть намного больше, чем при нарушении конфиденциальности;
- Частичное или полное нарушение работоспособности АСОИ (нарушение доступности, так как диапазон услуг, предоставляемых современными АСОИ, весьма широк, отказ в обслуживании может существенно повлиять на работу пользователя).

Рис.1.7. Внешняя и внутреняя безопасность АСОД

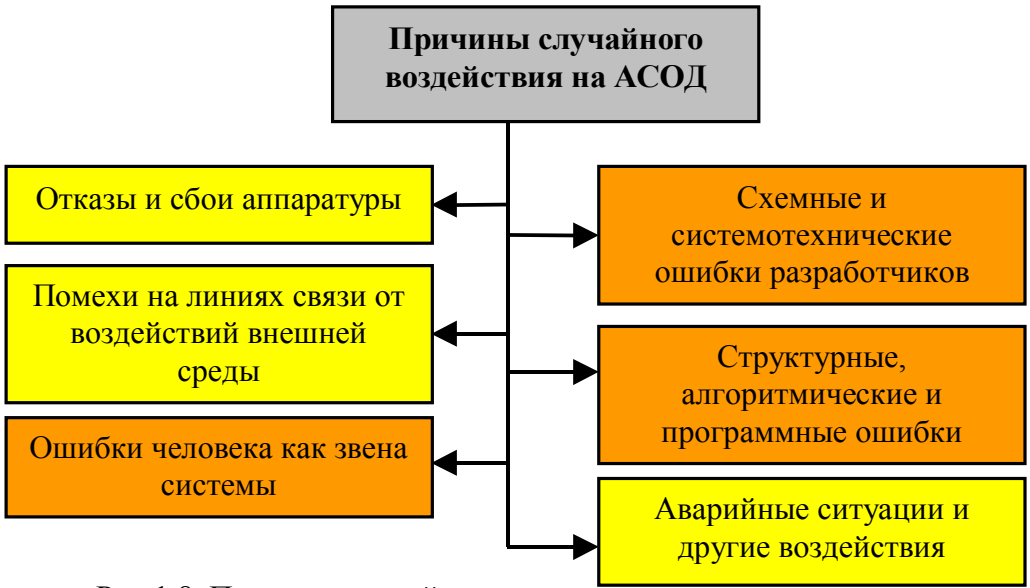


Рис.1.8. Причины случайных воздействий на АСОД

По принципу воздействия на АСОИ:

- С использованием доступа субъекта системы (пользователя, процесса) к объекту (файлу данных, каналу связи и т. д.). Под доступом понимается воздействие субъекта (выполнение некоторой операции) на объект приводящее к возникновению информационного потока от объекта к субъекту. При этом происходить взаимодействие субъекта и объекта и, следовательно, изменяется состояние объекта Воздействие, основанное на этом принципе проще, более информативнее и от нее легче защититься;
- С использованием скрытых каналов. Под скрытым каналом понимается путь передачи информации, позволяющий двум взаимодействующим процессам обмениваться информацией таким образом, который нарушает системную политику безопасности. При этом используются лишь побочные эффекты от взаимодействия двух субъектов,что не оказывает влияние на состояние системы. Здесь воздействие организовывать относительно трудно, принцип отличается меньшей информативностью и сложностью обнаружения и устранения. Эти каналы бывают двух типов:
  - скрытые каналы с памятью (позволяющие произвести чтение или запись информации другого процесса непосредственно или с помощью промежуточных объектов для хранения информации – временная память);
  - скрытые временные каналы (один процесс может получать информацию о действиях другого процесса, используя интервалы между какими-либо событиями – например, интервал времени между началом и концом процесса ввода-вывода дает информацию о размере вводимой или выводимой информации).

По характеру воздействия на АСОИ:

- активное воздействие (всегда связано с выполнением пользователем каких-либо действий, выходящих за рамки его обязанностей и нарушающих существующую политику безопасности – доступ к определенным наборам данных, программам, вскрытие пароля и т. д.). В результате изменяется состояние системы (осуществляется с использованием доступа и /или с использованием доступа и скрытых каналов);
- пассивное воздействие (осуществляется путем наблюдения каких-либо побочных эффектов и их анализа – например, подслушивание линии связи между двумя узлами сети). При этом всегда нарушается только конфиденциальность информации (так как при нем никаких действий с объектами и субъектами не производится) и состояние системы не изменяется.

По причине появления используемой ошибки защиты. Реализация какой-либо угрозы становится возможным, если в системе имеется ошибка или брешь в защите. Ошибка может быть обусловлена одной из следующих причин:

- Неадекватность политики безопасности реальной АСОИ (разработанная для данной системы политика безопасности настолько не отражает реальные аспекты обработки информации, что становится возможным использование этого несоответствия для выполнения несанкционированных действий). Модель никогда не может точно соответствовать реальной системе, но в одних случаях это не может приводить к нарушениям, а в других – может. Даже такие действия нельзя назвать несанкционированными, поскольку защита от них непредусмотрена политикой безопасности и система защиты в принципе не способна их предотвратить (необходимо разработать новую политику безопасности);
- Ошибки административного управления, под которыми понимается некорректная реализация или поддержка принятой политики безопасности в данной системе (например, неправильное определение прав доступа к определенным наборам данных);
- Ошибки в алгоритмах программ, в связях между ними и т. д., которые возникают на этапе проектирования программных продуктов и благодаря которым их можно использовать совсем не так, как описано в документации (например, ошибка в программе аутентификации пользователя системой, что дает возможность при помощи отдельных действий пользователю войти в систему без пароля).
- Ошибки реализации программ (ошибки кодирования), связей между ними и т. д., которые возникают на этапе реализации или отладки и которые могут служить источником недокументированных свойств (например, люки, которые обнаружить труднее всего).

По способу активного воздействия на объект атаки:

- Непосредственное воздействие на объект атаки, в том числе с использованием привилегий (например, непосредственный доступ к набору данных, программе, службе, каналу связи и т. д., воспользовавшись какой-либо ошибкой (нужно применить контроль доступа);
- Воздействие на систему разрешений, в том числе с захватом привилегий (здесь несанкционированные действия выполняются относительно прав пользователей, а сам доступ к объекту потом осуществляется законным образом – например, захват привилегий);
- Опосредованное воздействие через других пользователей;
- “маскарад” (пользователь присваивает себе каким-либо образом полномочия другого, выдавая себя за него;
- “Использование вслепую” (один пользователь заставляет другого выполнить необходимые действия, которые для системы защиты не выглядят несанкционированными – для этой угрозы может использоваться вирус, который выполняет необходимые действия и сообщает тому, кто его внедрил о результате). Для предотвращения подобных действий тре-

буется постоянный контроль за работой АСОИ в целом и со стороны пользователей за своими наборами данных.

Рис.1.9. Угрозы безопасности АСОД
(продолжение на следующей странице)

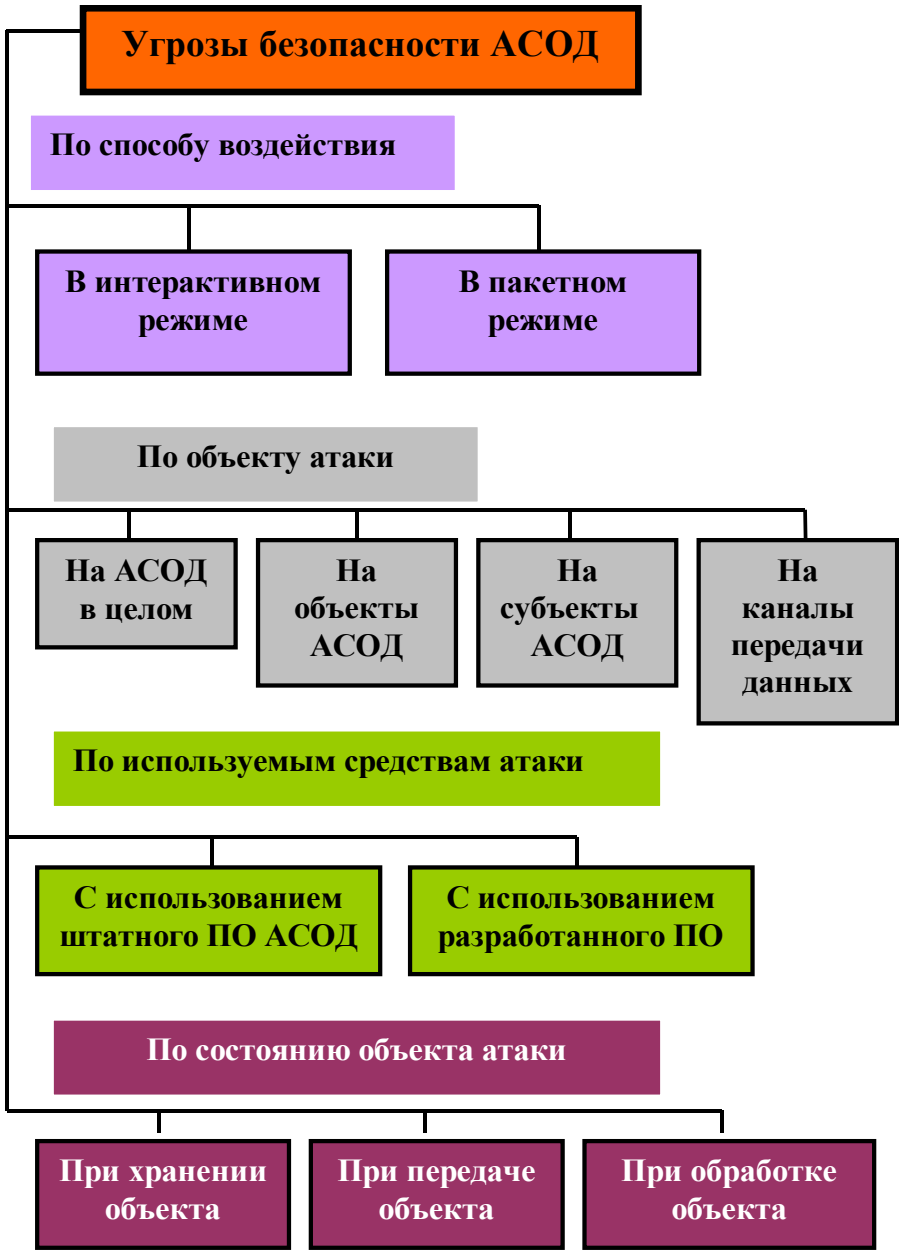


Рис.1.9 (конец). Угрозы безопасности АСОД

По способу воздействия на АСОИ:

- В интерактивном режиме (например, атака на систему при помощи интерпретатора команд – воздействие оказывается более длительным по времени и, может быть обнаружен но является более гибким);
- В пакетном режиме (например, с помощью вирусов – действие является кратковременным, трудно диагностируемым, более опасным, но требует большой предварительной подготовки, так как необходимо предусмотреть все возможные последствия вмешательства).

По объекту атаки:

- АСОИ в целом (для этого используются “маскарад”, перехват или подделка пароля, взлом или доступ к АСОИ через сеть);
- Объекты АСОИ (на программы в оперативной памяти или на внешних носителях, на сами устройства системы, на каналы передачи данных и т.

д. – получение доступа к содержимому носителей информации или нарушение их функциональности);

- Субъекты АСОИ – процессы и подпроцессы пользователей (цели: приостановка; изменение привилегий или характеристик; использование злоумышленником привилегий или характеристик и т. д.);
- Каналы передачи данных – передаваемые по каналу связи пакеты данных и сами каналы (нарушение конфиденциальности, подмена или модификация сообщений, нарушение целостности информации, изменение топологии и характеристик сети, нарушение доступности сети и т. д.).

По используемым средствам атаки:

- Использование стандартного программного обеспечения (ПО);
- Использование специально разработанных программ (поэтому в защищенных системах рекомендуется не допускать добавление программ в АСОИ без разрешения администратора безопасности системы).

По состоянию объекта атаки:

- Хранения (диск или другой вид носителя информации находится в пассивном состоянии – воздействие осуществляется с использованием доступа);
- Передачи по линиям связи между узлами сети или внутри узла;
- Обработки (объектом атаки является процесс пользователя).

Рассмотренный перечень еще раз подтверждает сложность определения возможных угроз и способов их реализации. Не существует и универсального способа защиты, который предотвратил бы любую угрозу. Следовательно необходимо объединить различные меры защиты для обеспечения безопасности всей АСОИ в целом.

В условиях массового использования ПЭВМ, открытых компьютерных сетей и общедоступных каналов связи существенно обострило проблему обеспечения безопасности информации.

В последнее время активно развивается ИНФОРМАЦИОННАЯ ИНТЕГРАЛЬНАЯ БЕЗОПАСНОСТЬ.

Под ИНФОРМАЦИОННОЙ ИНТЕГРАЛЬНОЙ БЕЗОПАСНОСТЬЮ понимается комплексная совокупность мер по защите информации в ходе всего непрерывного процесса подготовки, обработки, хранения и передачи информации (меры защиты действуют непрерывно в течении всего защищаемого периода – составляющие интегральной безопасности телекоммуникационных и информационно-вычислительных сетей приведены на рис.1.10).

Архитектура обеспечения безопасности связи эталонной модели взаимосвязи открытых систем (OSI) подробно разработана в международном консультативном комитете по телеграфии и телефонии (МКТТ) и изложена в его рекомендации X. 800 (необходимо защищать: информацию и данные – включая программную часть и пассивные данные по средствам защиты типа “паролей”; службу связи и обработки данных; оборудование и аппаратуру). Угроза системе передачи данных иллюстрируется на рис.1.11.

Рис.1.10. Составляющие информационной интегральной безопасности

Надлежащая СТРАТЕГИЯ ЗАЩИТЫ должна быть основана на аспектах той обстановки, которую считает важной ВЫСШЕЕ ЗВЕНО УПРАВЛЕНИЯ. Стратегия защиты трактуется в смысле “Что можно и что нельзя в плане защиты в процессе работы системы”. Она определяет наивысший уровень спецификации защиты (см. рис.1.12).

Характеристики защиты обычно повышают стоимость системы и могут усложнить ее эксплуатацию. Поэтому перед разработкой системы защиты необходимо определить тип угрозы, то есть произвести ОЦЕНКУ УГРОЗЫ. В общих чертах оценка системы сводится к следующему:

1. Определение степени уязвимости системы;
2. Оценка стоимости каждой попытки нарушения защиты;
3. Расчет потенциальных мер противодействия;
4. Выбор оптимального механизма защиты.

Полное техническое закрытие, как и физическое, невозможно. Задача состоит в том, чтобы сделать стоимость нарушения довольно высокой при приемлемых уровнях риска.

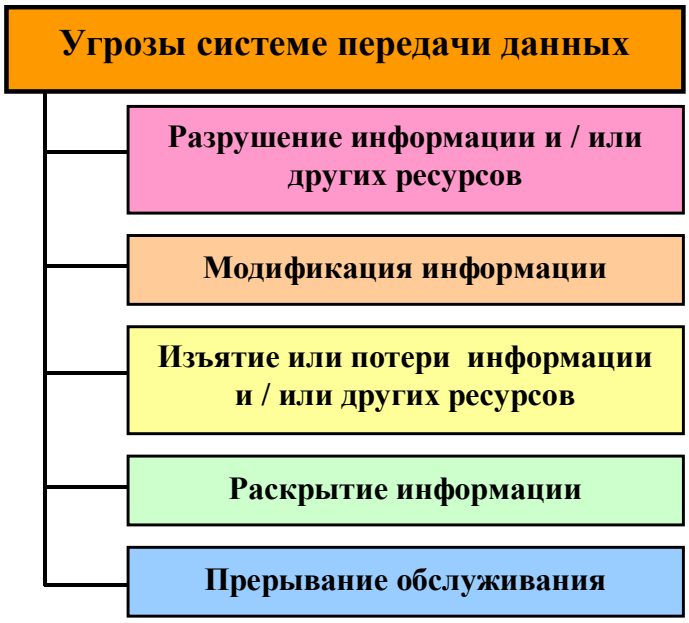


Рис.1.11. Угрозы системе передачи данных

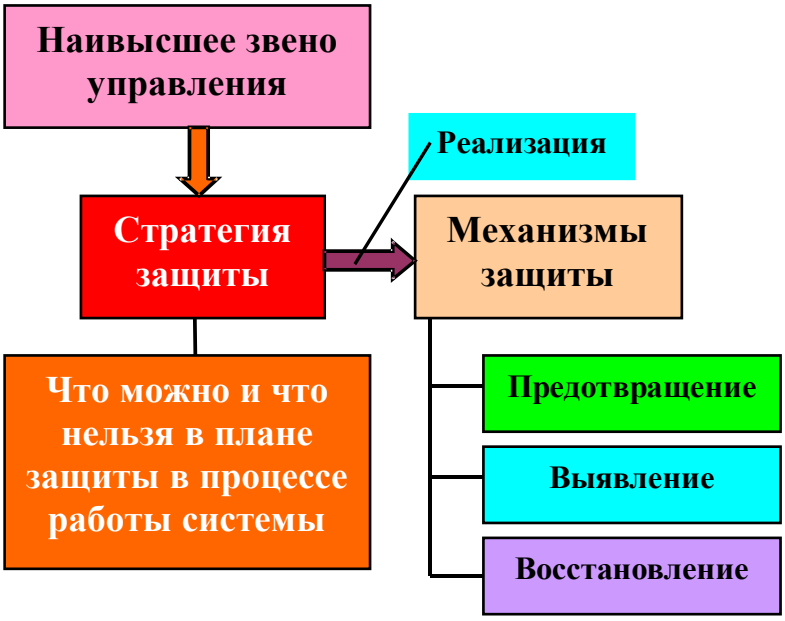


Рис.1.12. Назначение концепций защиты

Тема 5. МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОБРАБОТКИ ДАННЫХ

В последнее время активно развивается информационная интегральная безопасность.

Под информационной интегральной безопасностью понимается комплексная совокупность мер по защите информации в ходе всего непрерывного процесса подготовки, обработки, хранения и передачи информации (меры защиты действуют непрерывно в течении всего защищаемого).

Информационная интегральная безопасность делится на следующие составляющие:

- физическую безопасность (защита зданий, помещений, подвижных средств и т. д.);
- безопасность аппаратных средств (защита ЭВМ, сетевого оборудования и т.д.);
- безопасность программного обеспечения (защита программ от вирусов, "троянских коней", атак хакеров и т.д.);
- безопасность сети в целом (использование дополнительных мер защиты, вызванных особенность сети);
- безопасность связи (защита каналов связи от внешних воздействия любого вида).

Архитектура обеспечения безопасности связи эталонной модели взаимосвязи открытых систем (OSI) подробно разработана в международном консультативном комитете по телеграфии и телефонии (МКТТ) и изложена в его рекомендации X. 800 (необходимо защищать: информацию и данные – включая программную часть и пассивные данные по средствам защиты типа "паролей"; службу связи и обработки данных; оборудование и аппаратуру).

Угроза системе передачи данных можно классифицировать следующим образом:

- разрушение информации и / или других ресурсов;
- модификация информации;
- модификация информации;
- раскрытие информации;
- прерывание обслуживания.

Надлежащая стратегия защиты должна быть основана на аспектах той обстановки, которую считает важной высшее звено управления. Стратегия защиты трактуется в смысле “Что можно и что нельзя в плане защиты в процессе работы системы”. Она определяет наивысший уровень спецификации защиты.

Характеристики защиты обычно повышают стоимость системы и могут усложнить ее эксплуатацию. Поэтому перед разработкой системы защиты необходимо определить тип угрозы, то есть произвести ОЦЕНКУ УГРОЗЫ. В общих чертах оценка системы сводится к следующему:

1) определение степени уязвимости системы;
2) оценка стоимости каждой попытки нарушения защиты;
3) расчет потенциальных мер противодействия;
4) выбор оптимального механизма защиты.

Полное техническое закрытие, как и физическое, невозможно. Задача состоит в том, чтобы сделать стоимость нарушения довольно высокой при приемлемых уровнях риска.

Основные методы защиты информации, применяемые в АСОД

При наличии относительно простых средств обработки, хранения и передачи информации существовали, и до настоящего времени не потеряли свое значение, определенные методы защиты от преднамеренного доступа (см. рис.2.1).

Относительно простые методы защиты от преднамеренного доступа:

- ограничение доступа;
- разграничение доступа;
- криптографическое преобразование информации;
- контроль и учет доступа;
- разделение доступа (привилегий);
- законодательные меры.

Перечисленные методы осуществлялись чисто организационно или с помощью технических средств.

С усложнением технических средств и развитием различных сетей, с увеличением объемов обрабатываемой информации и количества пользователей возросла вероятность несанкционированного доступа к информации. Этому также способствует увеличение количества и видов случайных воздействий и каналов несанкционированного доступа. Следовательно, развиваются старые и появляются новые методы защиты информации в вычислительных системах, такие как:

- методы повышения достоверности информации;
- методы защиты информации от аварийных ситуаций;
- методы контроля доступа к внутреннему монтажу аппаратуры, линиям связи и технологическим органам управления;
- методы разграничения и контроля доступа к информации;
- методы защиты от побочного излучения и наводок информации;
- методы идентификации и аутентификации пользователей, технических средств, носителей информации и документов.

ОГРАНИЧЕНИЕ ДОСТУПА. Создание вокруг объекта защиты некоторой физически замкнутой преграды с организацией контролируемого доступа лиц, связанных с объектом по своим функциональным обязанностям (применяются различные датчики, организуется система охранной сигнализации).

КОНТРОЛЬ ДОСТУПА К АППАРАТУРЕ. Внутренний монтаж аппаратуры, технологические органы и пульты управления закрыты физически определенными средствами, на которые установлены датчики. Датчики соответствующими цепями соединяются с централизованным устройством контроля. Этот тип контроля также способствует соблюдению технологической дисциплины в целях обеспечения нормального функционирования вычислительной системы. С позиций защиты информации от несанкционированного доступа (НСД) контроль вскрытия аппаратуры защищает от следующих действий:

- изменения и разрушения схемы вычислительной системы и аппаратуры;
- подключения постороннего устройства;
- изменения алгоритма работы системы (с использованием технологических пультов и органов управления);
- загрузки посторонних программ и внесения программных “вирусов” в систему;
- использования терминалов посторонними лицами и т. д.

Доступ к штатным входам в систему (ТЕРМИНАЛАМ) обеспечивается выдачей механических ключей пользователям. Доступ же к самой информации обеспечивается с помощью системы опознания и разграничения доступа, включающей применения кодов паролей и специального терминала службы безопасности информации.

РАЗГРАНИЧЕНИЕ И КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИИ В АСОИУ. Сущность этого метода состоит в том, что осуществляется разделение циркулирующей в системе информации на определенные части, а доступ к последним организуется в соответствии с функциональными обязанностями и полномочиями должностных лиц. Основной задачей разграничения доступа является сокращение количества должностных лиц, не имеющих отношение к определенным частям информации при выполнении своих функций (защита информации от нарушителя среди допущенного к ней персонала). Деление информации может производиться по степени важности, секретности, по функциональному назначению и т. д. Так как доступ осуществляется с различных технических средств, то целесообразно разграничение начинать с размещения этих средств в раздельных помещениях. Основные задачи системы должны быть технически и организационно отделены от подготовительных функций технического обслуживания аппаратуры, ее профилактики, перезагрузки программного обеспечения и т. д. Комплекс средств автоматизации (КСА) и организация его обслуживания организуется следующим образом:

1) техническое обслуживание КСА в процессе эксплуатации должна выполняться отдельным персоналом без доступа к информации, подлежащей защите;

2) перегрузка программного обеспечения и всякие ее изменения должны производиться специально выделенным для этой цели проверенным специалистом;

3) функции обеспечения безопасности информации должны выполняться специальным подразделением в организации;

4) организация доступа пользователей к памяти КСА должна обеспечиваться с разграничением доступа к информации, хранящейся в ней, с достаточной степенью детализации и в соответствии с заданными уровнями полномочий пользователей;

5) процессы регистрации и документирования технологической и организационной информации должны быть разделены.

Во имя достижения указанных целей при проектировании базового вычислительного комплекса (ВК) для построения КСА осуществляется следующее:

- разработка операционной системы с возможностью реализации разграничения доступа к информации, хранящейся в памяти ВК;
- изоляция областей доступа;
- разделение базы данных на группы;
- осуществления процедур контроля пересиленных ранее функций.

При проектировании самого КСА и информационной системы для АСОИУ (сети) на его базе выполняются следующие работы:

- разработка и реализация функциональных задач по разграничению и контролю доступа к аппаратуре и информации как в рамках данного КСА, так и АСОД (сети) в целом;

- разработка аппаратных средств идентификации и аутентификации пользователя;

- разработка программных средств контроля и управления разграничением доступа;

- разработка отдельной эксплуатационной документации на средства идентификации, аутентификации, разграничения и контроля доступа

РАЗДЕЛЕНИЕ ПРИВИЛЕГИЙ НА ДОСТУП. Этот метод основывается на том, что образуется допущенная к информации группа должностных лиц и на нее распространяется следующее условие: доступ к информации получает вся группа целиком если все члены группы одновременно предъявили свои полномочия на нее (при этом существенно затрудняется преднамеренный перехват информации нарушителем). Это похоже на сейф с несколькими ключами. Метод хотя и усложняет процедуру, но одновременно обладает высокой эффективностью. На этом принципе можно организовать доступ к данным с санкции вышестоящего лица. В некоторых случаях возможен вариант использования права на доступ к информации вышестоящего руководителя только при наличии его идентификатора и идентификатора его заместителя или представителя службы безопасности информации. Тогда информация выдается толь руководителю, а подчиненному выдается толь информация о факте выдачи информации (см. рис.1).

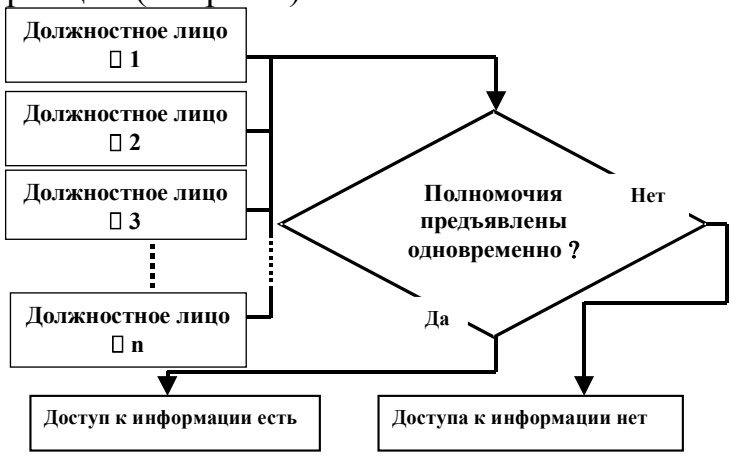


Рис.1. Разделение привилегий на доступ

ИДЕНТИФИКАЦИЯ И УСТАНОВЛЕНИЕ ПОДЛИННОСТИ ОБЪЕКТА (СУБЪЕКТА). В начале раскроем смысл понятий “идентификация” и “аутентификация” (см. рис 2).

При обмене информацией между человеком и ЭВМ желательно в любом случае предусмотреть взаимную проверку подлинности полномочий объекта или субъекта. Для этого необходимо, чтобы каждый из объектов (субъектов) хранил в своей памяти (недоступной для посторонних) список образов (имен)

объектов, с которыми будет производиться обмен информацией, подлежащей защите.

Перечислим основные методы, применяемые для установления подлинности различных объектов. Прежде всего, существует идентификация и установление подлинности:

- личности ("ключ-замок"; присвоение объекту уникального имени или ключа – ПАРОЛЯ и хранение его значения в ВС; разделение кода пароля на две части: запоминаемая пользователем и вводимая вручную; размещаемая на специальном носителе – карточке; "запрос-ответ"; "рукопожатие");

- технических средств (идентификация и установление подлинности терминала с использованием паролей, использование последних для установление подлинности ЭВМ по отношению к пользователю и т. д.);

- документов (применение криптографического преобразования информации является эффективным средством в сетях использование цифровой подписи и обеспечивающих защиту каждой стороны осуществляется введением специальных протоколов).

ИДЕНТИФИКАЦИЯ И УСТАНОВЛЕНИЕ ПОДЛИННОСТИ ЛИЧНОСТИ. Вообще идентификатором личности является его внешний вид: черты лица, форма головы, фигура, характер и другие свойственные данному человеку признаки. Эти признаки образ конкретного человека. По этим признакам мы или узнаем или не узнаем нашего знакомого. Некоторые признаки носят индивидуальный характер и они не изменяются всю жизнь (отпечатка пальцев, тембр голоса, личная подпись и т. д.). Часть признаков со временем меняется. У каждого человека эти признаки формируют различные образы одного и того же человека (некоторые признаки совпадают, некоторые нет). Эти обстоятельства и трудности технической реализации средств идентификации указанных признаков заставляют искать иные пути решения задачи идентификации личности.

При разработке систем распознавания образов ставится задача повысить точность воспроизведения образа с целью автоматически отобрать из множества потенциальных образов единственный, хранящийся в памяти системы. Мощность этого множества приближается к бесконечности и по этому, и по ряду других причин применение систем распознавания образов для защиты информации в ВС видимо нецелесообразно.

Система “ключ – замок” является простой и распространенной системой аутентификации. Владелец ключа является объектом установления подлинности. Однако ключ можно потерять, похитить и т. д., так как идентификатор личности от нее отделен. Эта система в сочетании с другими, в условиях пониженных требований применяется до сих пор.

Наиболее распространенный метод аутентификации заключается в присвоении лицу или другому объекту уникального имени или числа – пароля и хранения его значения в ВС (см. рис.3).

Рис.2. Идентификация и установление подлинности субъекта (объекта)

Более высокий уровень безопасности входа в систему достигается при разделении кода пароля на две части (одна часть запоминается пользователем и вводится вручную, а другая хранится на специальном носителе – карточке, которая связана с терминалом). В этом случае при хищении карточки будет время для замены пароля и получения новой карточки. Для случая когда нарушитель путем физического принуждения все таки получит запоминаемую часть пароля, можно предусмотреть систему тревожной сигнализации (наличие ложного пароля и выдачи его).

Имеется метод “запрос – ответ” в котором используется набор ответов на некоторое количество стандартных вопросов и определенное количество ответов на вопросы, ориентированные на пользователя. Эти вопросы и ответы хранятся в памяти ЭВМ и управляются операционной системой. При попытке вхождения пользователя в систему операционная система задает ему в определенном порядке эти вопросы и при правильных ответах допускает к работе.

Рис.3 Применение КРИПТОГРАФИЧЕСКОГО

С целью исключения некоторых недостатков выше описанных методов операционная система может потребовать, чтобы пользователь доказал свою подлинность корректной обработкой некоторых алгоритмов. Эту часть называют процедурой в режиме “рукопожатия” (она может быть выполнена как между ЭВМ и пользователем, так и между двумя ЭВМ).

ИДЕНТИФИКАЦИЯ И УСТАНОВЛЕНИЕ ПОДЛИННОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ. Здесь широко используются пароли как для идентификации и установления подлинности терминала, с которого пользователь входит в систему, так и для обратного установлении подлинности ЭВМ по отношению к пользователю.

ИДЕНТИФИКАЦИЯ И УСТАНОВЛЕНИЕ ПОДЛИННОСТИ ДОКУМЕНТОВ. Подлинность документов необходимо рассматривать со следующих позиций: документ сформирован непосредственно в этой ВС на его аппаратуре документирования; документ получен с удаленных объектов.

В первом случае подлинность документа гарантируется средствами защиты информации от НСД и применением криптографического преобразования информации. Информация закрывается кодом пароля (он известен передающему лицу и получателю).

Во втором случае опять таки широко используется криптографическое преобразование информации (документ относительно долго хранился или транспортировался по неохраняемой территории). Используется также цифровая подпись. Подпись сообщения представляет собой способ шифрования сообщения с помощью криптографического преобразования. Закрываемым

элементом в преобразовании является код ключа. Ключ подписи принадлежит конечному множеству ключей (множество достаточно велико). Ключ подписи определяется случайным выбором. Практически подпись является паролем, зависящим от отправителя, получателя и содержания передаваемого сообщения. Для предупреждения повторного использования подпись должна меняться от сообщения к сообщению.

ИДЕНТИФИКАЦИЯ И УСТАНОВЛЕНИЕ ПОДЛИННОСТИ ИНФОРМАЦИИ НА СРЕДСТВАХ ЕЕ ОТОБРАЖЕНИЯ И ПЕЧАТИ. Подлинность информации на средствах ее отображения тесно связана с подлинностью документов и поэтому все соображения по отношению к определению подлинности документов относятся также и к подлинности информации, отображаемой на средствах отображения. Здесь также используется криптографическое преобразование информации.

Тема 6. КРИПТОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ

Криптографические методы преобразования информации являются одним из эффективных методов, значительно повышающих безопасность передачи данных в сетях ЭВМ, а также данных, хранящихся в удаленных устройствах памяти и при обмене информацией между удаленными объектами. Суть криптографического преобразования информации иллюстрируется на рис.1. Знание ключа позволяет расшифровать текст, а не знание его этот процесс практически делает невыполнимым даже при известном алгоритме преобразовании.

Для получения из шифрованной информации оригинал применяется обратный процесс – дешифрование. Между кодированием и шифрованием принципиальной разницы нет. В последнее время на практике процесс, который выполняется с целью получения цифрового представления информации для ее дальнейшей обработки на технических средствах называется кодированием (обратный процесс – декодированием). А процесс преобразования информации с целью ее защиты от несанкционированного доступа называется шифрованием (обратный процесс – дешифрование).

Современные методы защитных криптографических преобразований делятся на методы:

- перестановки;
- подстановки (замены);
- аддитивные;
- комбинированные.

Само шифрование может быть симметричным и несимметричным.

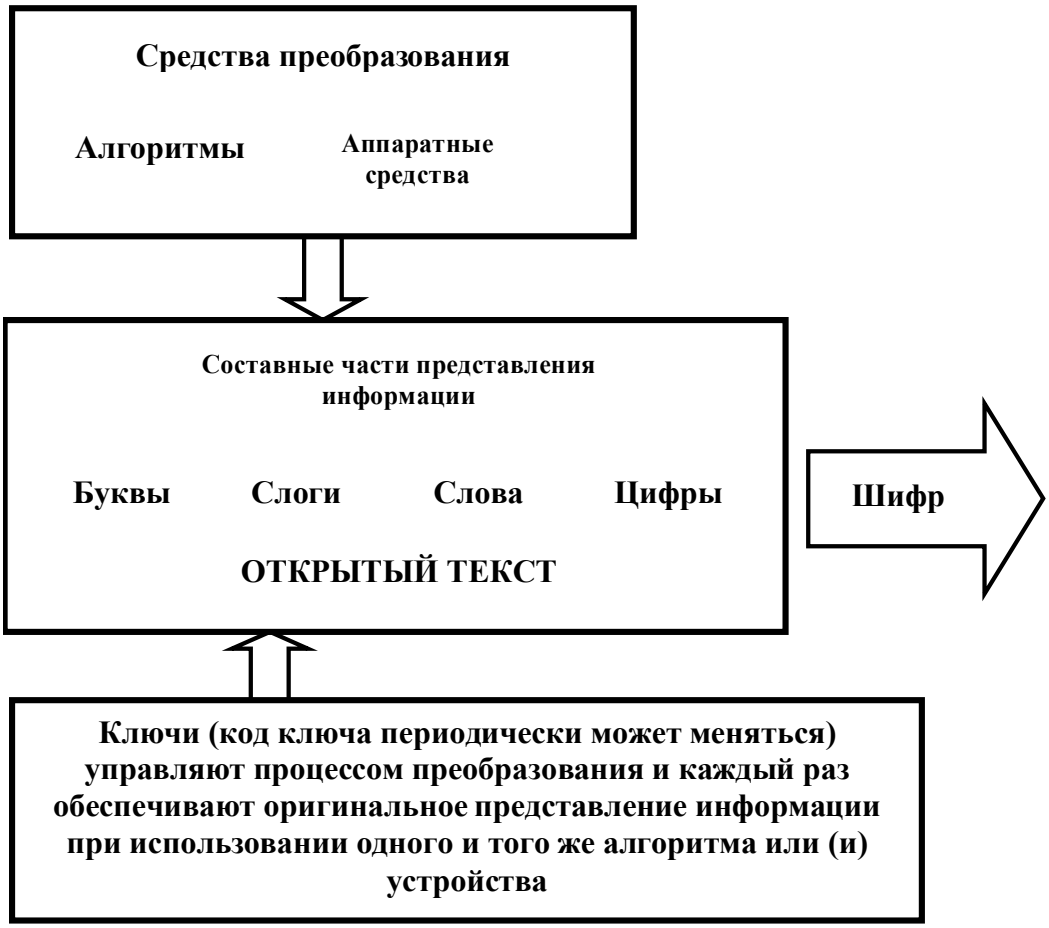


Рис.1. Составляющие процесса криптографического преобразования (шифрование, кодирование) информации

Перед методами защитного преобразования информации ставятся следующие основные требования: достаточная устойчивость к попыткам раскрытия зашифрованного текста; объем ключа не должен затруднять его запоминание и пересылку; алгоритм преобразования информации, а также ключ (используемый для шифрования и дешифрования) не должны быть очень сложным; ошибки в шифровании не должны вызывать потерю информации; длина зашифрованного текста не должна на много превышать длину исходного текста; временные и стоимостные ресурсы, требуемые для процессов преобразования информации должны определяться требуемой степенью защиты информации.

Методы перестановки.

Суть метода перестановки иллюстрируется на рис.2.

Простым примером перестановки может быть запись исходного текста по столбцам и чтение шифрованного текста по строкам. Например, если исходный текст состоит из следующего

НЕЯСНОЕ СТАНОВИТСЯ ЕЩЕ БОЛЕЕ НЕПОНЯТНЫМ

Рис.2. Суть метода перестановки

и записать его в матрицу по столбцам (матрица состоит из 5 строк и 7 столбцов), то получим

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Если текст в матрице прочитать по строкам с разбиением на группы (в каждой группе по 5 букв), то получим зашифрованный текст

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ
ЕОЫНА ТЕЕНМ

Более практичный метод шифрования, называемый одиночной перестановкой по ключу очень похож на предыдущий. Здесь столбцы матрицы переставляются по ключевому слову. Число букв в ключевом слове равно количеству столбцов матрицы. Буквы ключевого слова нумеруются по их естественному порядку в алфавите (если в ключе имеются повторяющиеся буквы, то они нумеровались бы слева направо. Рассмотрим еще один пример (см. 3), называемый методом одиночной перестановки.

Характерным для методов перестановки является то, что у них алгоритмы преобразования относительно просты, они легко программно и аппаратно реализуемы, однако имеют относительно низкий уровень защиты.

Методы замены (подстановки).

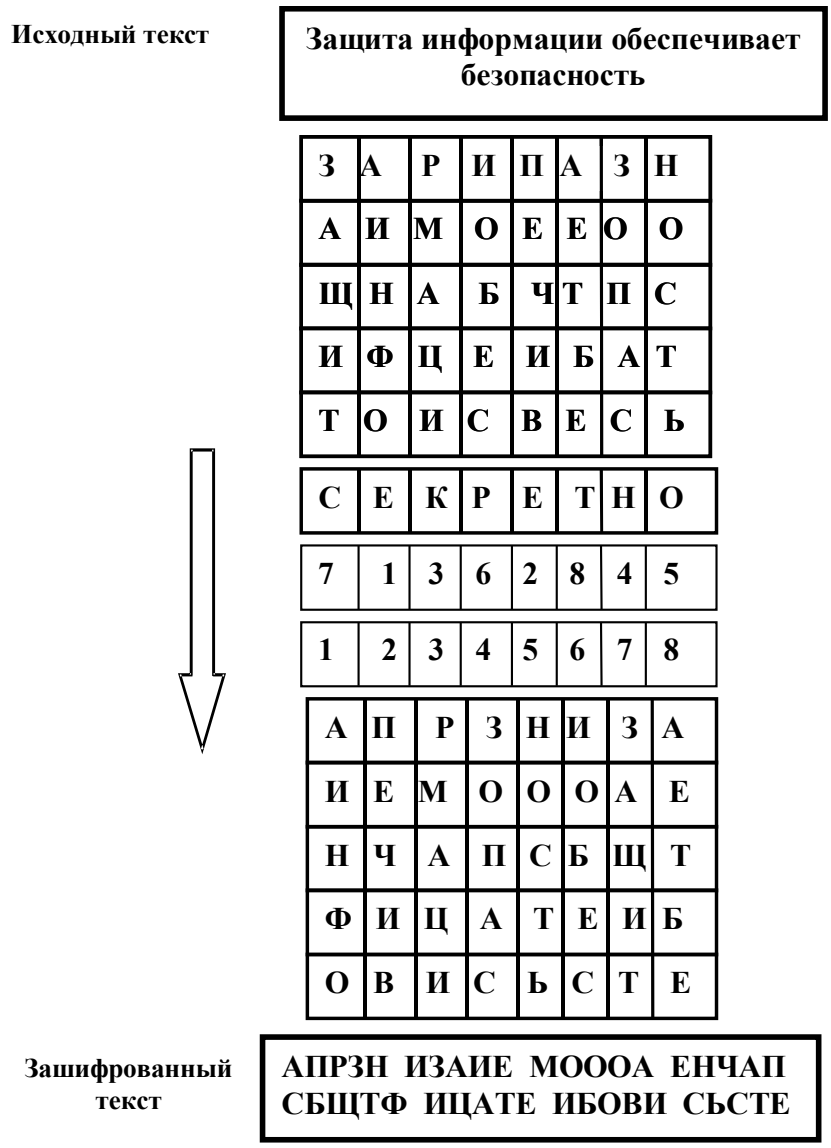


Рис.3. Пример метода одиночной перестановки

Суть метода замены (подстановки) иллюстрируется на рис. 4.

Простейшим методом из этого множества методов является прямая замена исходных символов их эквивалентами из вектора замен. Алгоритм прост: для очередного символа исходного текста определяется позиция его размещения в первичном алфавите (θ); эквивалентный символ вторичного алфавита определяется по вектору замен как смещение θ от начала вектора.

При дешифровании процесс выполняется в обратном направлении (вектор замен ⇒ первичный алфавит ⇒ эквивалентный символ первичного алфавита). Текст имеет относительно низкий уровень защиты, так как исходный и шифрованный тексты имеют одинаковые статистические характеристики.

Метод, использующий таблицу Вижинера отличается более высокой стойкостью. Таблица Вижинера в первой строке содержит все символы алфавита, размещенные в естественном порядке. Символы второй строки получаются из первой путем циклического сдвига последней на один символ влево (при этом первый символ первой строки оказывается последним символом второй строки).

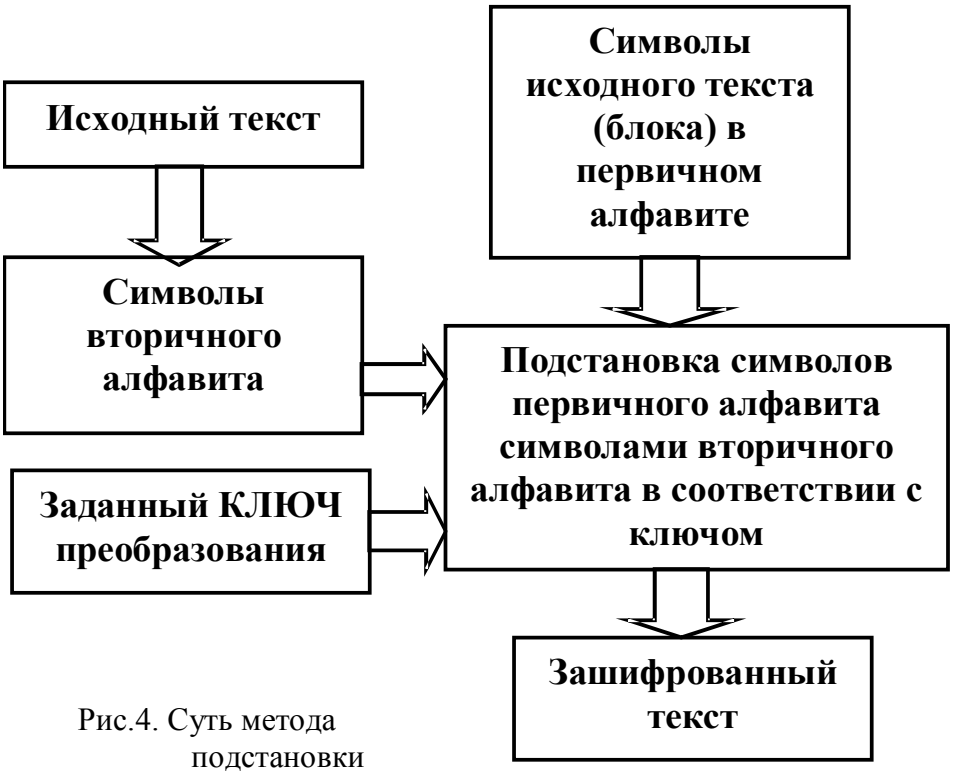


Рис.4. Суть метода подстановки

Таким образом формируется квадратная матрица размерности N, где N – количество символов первичного алфавита.

МАТРИЦА ВИЖИНЕРА
(ДЛЯ АЛФАВИТА РУССКОГО ЯЗЫКА)

АБВГДЕ……ЭЮЯ

БВГДЕЖ ЮЯА
ВГДЕЖЗ ЯАБ

ЯАБВГД ЬЭЮ

Для шифрования текста определяется ключ – некоторое слово или набор букв. Далее на базе матрицы Вижинера и ключа следующим образом формируется подматрица шифрования. В качестве первой строки подматрицы берется первая строка матрицы Вижинера. Остальные строки также выбираются из матрицы Вижинера в соответствии с последовательностью букв ключа. Алгоритм преобразования состоит из следующего.

1. Записывается шифруемый текст;
2. Начиная слева направо под шифруемым текстом записывается (символ под символом) ключ (он повторяется столько раз пока не накроет весь шифруемый текст);
3. Берется первая (очередная) буква (например, “Э”) шифруемого текста и определяется буква ключа под ней (например, “Ю”);
4. В подматрице выбирается строка в соответствии с буквой ключа (т. е. “Ю”);

5. Определяется позиция заменяемой буквы шифруемого текста в первой строке подматрицы (“Э”) и соответствующая буква на этой же позиции в строке подматрицы, определенной в п.4 (например, ”М”);

6. Заменяется буква “Э” на букву “М”;

7. Данный процесс побуквенной обработки шифруемого текста продолжается до достижения конца текста.

Рассмотрим следующий пример (см. рис. 5), который отражает последовательность выполняемых действий при использовании матрицы Вижинера для преобразовании исходного текста и получении шифрованного образа [ ].

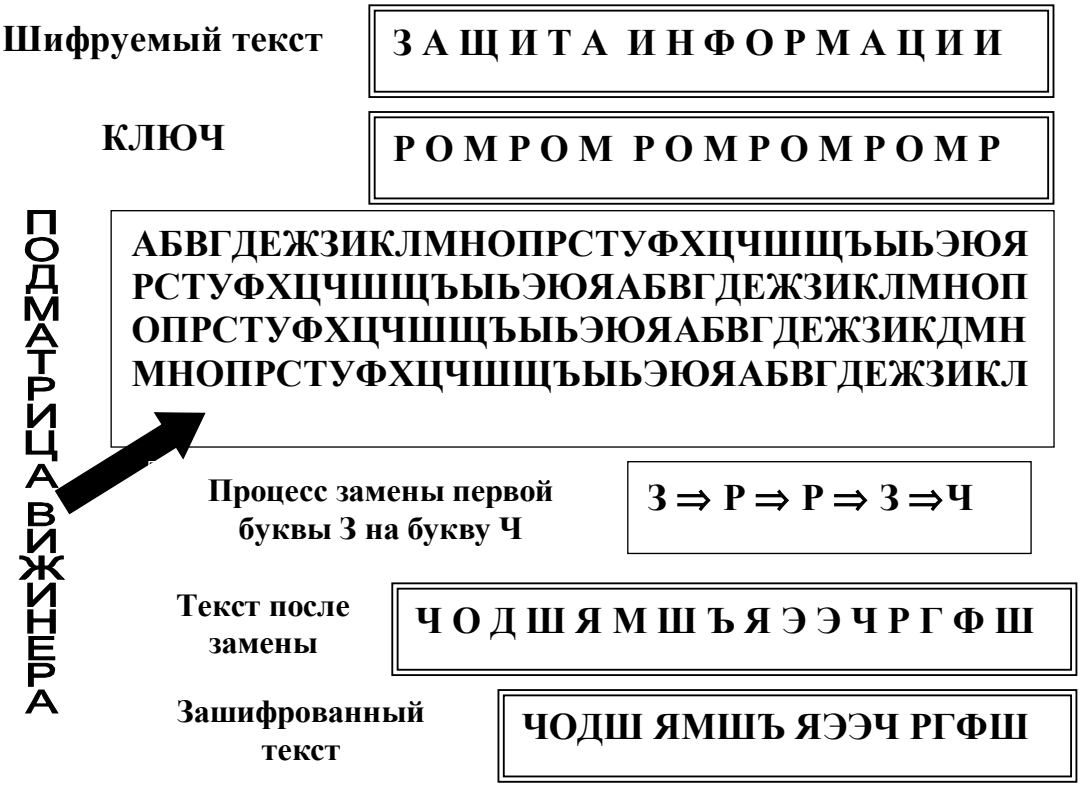


Рис.5. Пример метода подстановки с применением матрицы Вижинера

Процесс обратного преобразования происходит следующим образом:

1. Над буквами шифрованного текста последовательно записываются буквы ключа;

2. В строке подматрицы для каждой буквы ключа отыскивается буква, соответствующая символу шифрованного текста. Находящаяся над ней буква первой строки и будет символом шифрованного текста;

3. Полученная последовательность букв в конце группируются в слова по смыслу.

Недостатками этого метода являются: ненадежность шифрования при коротком ключе; сложность формирования длинных ключей; в ключе не должно быть повторяющихся букв; длинный ключ трудно запоминается.

С целью повышения эффективности метода разработаны его различные модификации. Существуют и другие методы подстановки.

Аддитивные методы.

Здесь в качестве ключа используется некоторая последовательность букв того же алфавита, в котором представлен исходный текст и равный по длине последнему. Сам процесс шифрования из суммирования исходного текста и ключа по модулю, равному числу букв в алфавите (например, по модулю 2, если алфавит двоичный).

Методы гаммирования – наложения на исходный текст некоторой последовательности кодов (ключа), называемой гаммой. Алгоритм приводится на рис. 6.

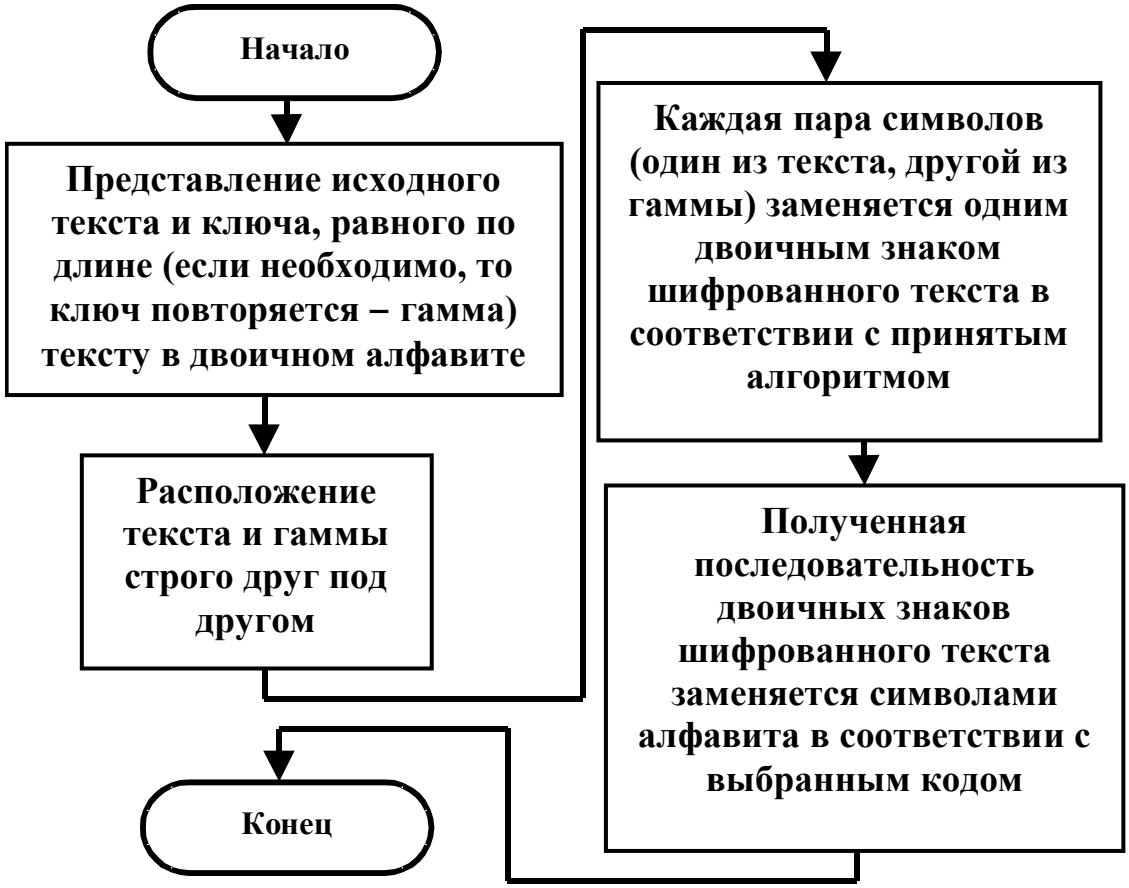


Рис. 6. Обобщенный алгоритм выполнения метода гаммирования

Если ключ будет подобран случайным образом (например, получен от датчика случайных чисел), то раскрыть шифрованный текст, не зная ключа, практически невозможно. Рассмотрим простой пример (см. рис. 7).

О выборе метода преобразования. Приведенные общие сведения о методах шифрования не претендуют на глубокий анализ и полноту. Хотелось бы также в общих чертах дать сведения о сравнении методов.

Все естественные и искусственные языки имеют присущие им частотные распределение букв своих алфавитов и других знаков. Эти характеристики вносят свои особенности в различные методы шифрования.

Рис. 7. Пример шифрования цифрового текста по методу гаммирования

Например, многие сообщения, зашифрованные методами перестановки или одноалфавитной подстановки сохраняют свои характерные частотные распределения и, таким образом, дают криптоаналитику ключ к раскрытию шифра (имеется так называемый индекс соответствия (ИС) для каждого языка, который для криптоаналитиков дает возможность определить правильный путь проводимых исследований по раскрытию шифра). Например для английского языка ИС определяется следующим образом

$$[(N-m)/(m*(N-1))]*0.066+0.038*[(N*(m-1)/(m*(N-1)],$$

где N – длина сообщения в буквах; m – число алфавитов.

Например, шифровки, дающие значения ИС, большие, чем 0.066 говорят о том, что вероятно использовалась одноалфавитная подстановка и т. д.

Большую роль играет значение характеристики, определяемой как отношение длины ключа к длине закрываемого им текста. Если значение этой характеристики ближе к единице, то значит шифровка более надежна. Опасность использования короткого ключа покажем на предыдущем примере (см. рис. 8). Как видно из анализа примера, для повышения эффективности шифрования необходимо применять длинные ключи, что в свою очередь порождает свои определенные трудности.

Эффективным способом установления ключа является применение генераторов случайных чисел (уравнения генератора псевдослучайных чисел).

Комбинированные методы шифрования . Комбинируя методы перестановки и подстановки получают метод преобразования, называемый шифрование произвольным шрифтом. Получаемый шифр обладает более сильными криптографическими возможностями. Он используется в федеральном стандарте NBS США, НАЗЫВАЕМОМ ТАКЖЕ СТАНДАРТОМ DES (в отечественном ГОСТе 28147–89, введен в действие с июля 1990 г.).

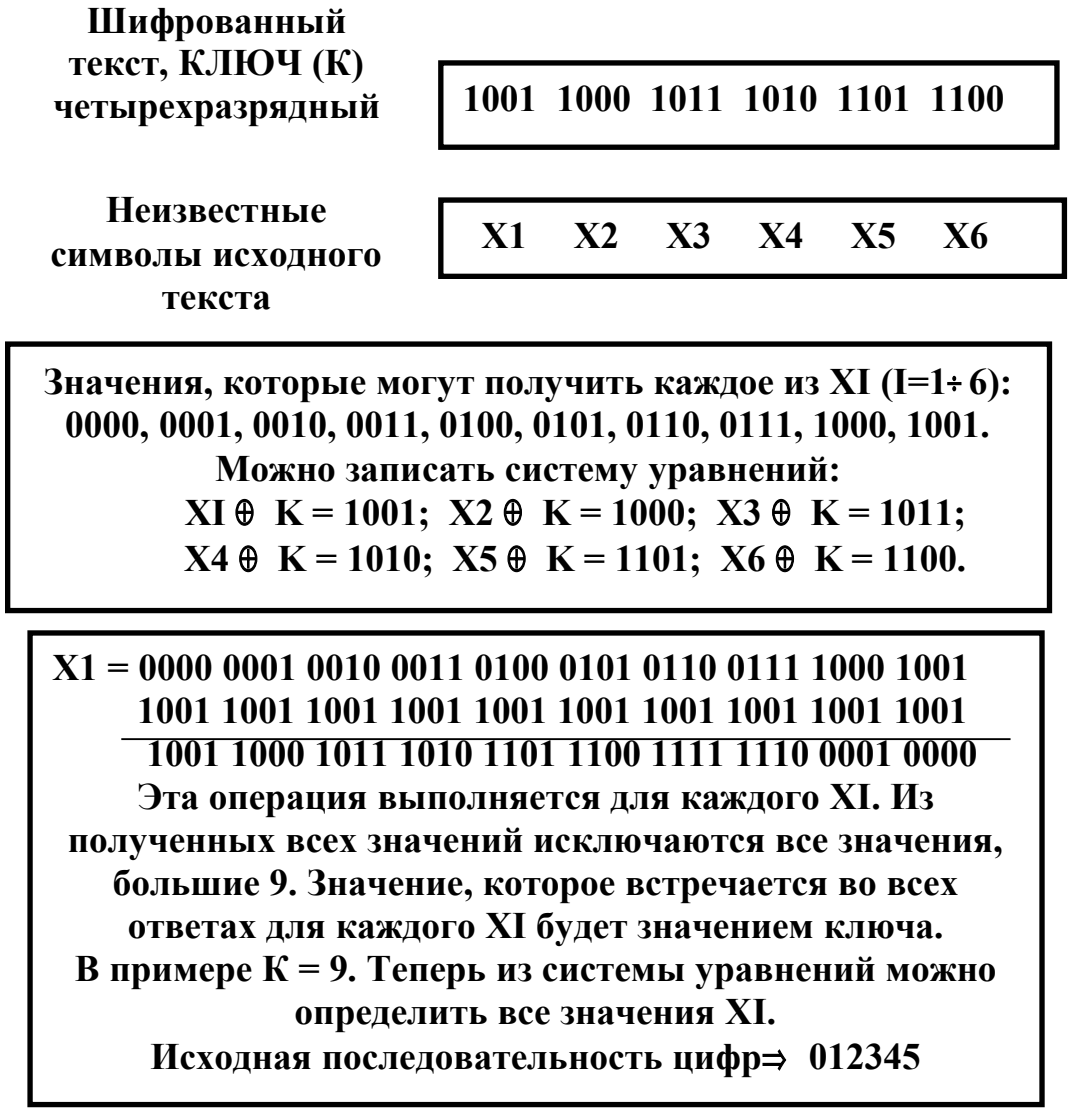


Рис. 8. Расшифровка значения короткого ключа в методе гаммирования

DES построен на комбинированном использовании методов перестановки, подстановки и гаммирования (каждый блок, длиной 32 бита каждый последовательно подвергается 15-кратному преобразованию). В качестве ключа, который используется для генерирования последовательности знаков случайной гаммы , используется последовательность в 56 бит (10^{16} различных комбинаций гаммы). Наиболее широко DES используется для хранения и передачи данных в ВС, в почтовых системах и т. д. С помощью алгоритма DES можно зашифровать файлы ЭВМ для их хранения. DES стал наиболее признанным механизмом криптографической защиты несекретных данных для массового применения. Он имеет различное исполнение (скоростные по-

казатели – свыше 100000 бит/с для компьютера VAX 780, до 20000 бит/с для ПК). К алгоритму шифрования предъявляются следующие требования (см. рис.9).

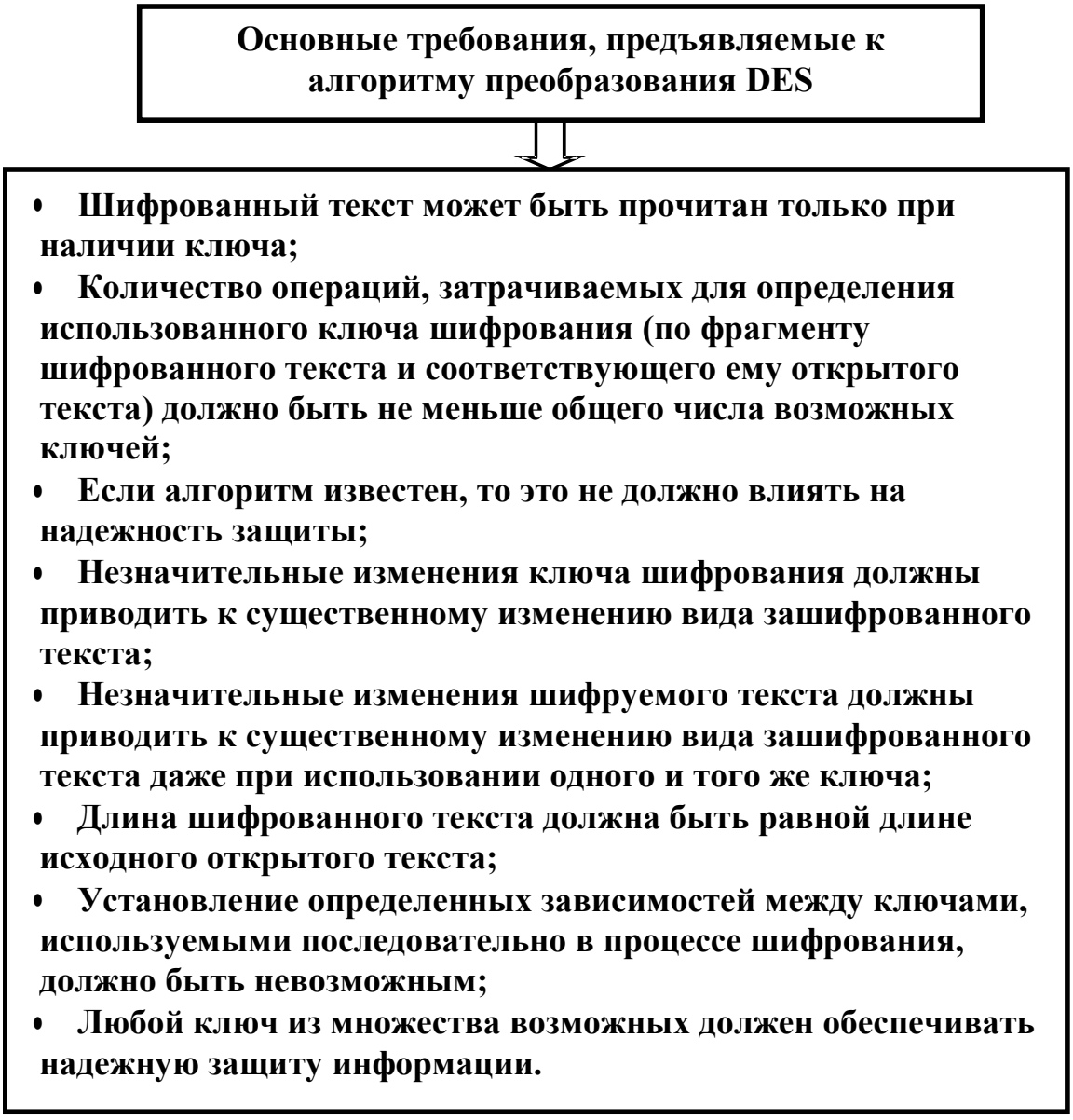


Рис.9. Некоторые требования, предъявляемые DES

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация имеет свои преимущества (высокая производительность и упрощенная организация обработки информации.

DES (Data Encryption Algorithm) введен в действие с 1977-го года и, помимо всего, широко применяется в банковской сфере (ISO 8731 – 1/ANSI 83. 92).

Аналогичный стандарт криптографического преобразования в России (отмеченный ранее ГОСТ 28147-89) был введен в 1990-ом году. Он не накладывает ограничения на степень секретности обрабатываемой информации. Это блочный алгоритм с секретным ключом. Шифрования данных производится блоками, размер которых выбирается шифровальщиком. Для шифрования и расшифрование производится тем же ключом. Последний шифруемый

блок может иметь длину на 8 байт меньше. Длина ключа составляет 256 бит. Длина блока подставки составляет 512 бит (минимальная длина блока составляет 64 бита). Стойкость алгоритма превосходит стойкость DES.

Существенным недостатком данного стандарта является сложность его программно-аппаратной реализации и, как следствие этого, низкая скорость шифрования данных.

Для проверки соответствия алгоритма и его реализации ФАПСИ проводится сертификация (например, сертификат имеет плата “Криптон-3”).

Системы с открытым ключом. В традиционных криптосистемах одним и тем же секретным ключом осуществляется как шифрование, так и расшифрование сообщения. Это предполагает, что отправитель и получатель сообщения получили идентичные копии ключа. При шифровании с открытым ключом для шифрования и дешифрирования используются разные ключи (см. рис.10).

Криптографические системы с открытым ключом основываются на необратимых или односторонних функциях (например, алгоритм RSA основывается на трудности разложения очень больших целых чисел на простые сомножители). Исследования необратимых функций проводятся в основном по трем направлениям: дискретное возведение в степень; умножение простых чисел; комбинаторные задачи. Криптография с открытым ключом применяется для шифрования передаваемых данных, при замены обычной подписи цифровой подписью, в системах электронных платежей и т. д. Уже имеются соответствующие технические средства (система SEEK, выпускаемая в составе шифрующей аппаратуры фирмой Cylink).

Появился новый алгоритм IDIA (International Data Encryption Algorithm) –алгоритм блочного шифрования, блоки открытого текста длиной64 бита, шифрованный текст такой же длины, длина ключа шифрования 128 бит, для шифрования и дешифрования используется один и тот же алгоритм.

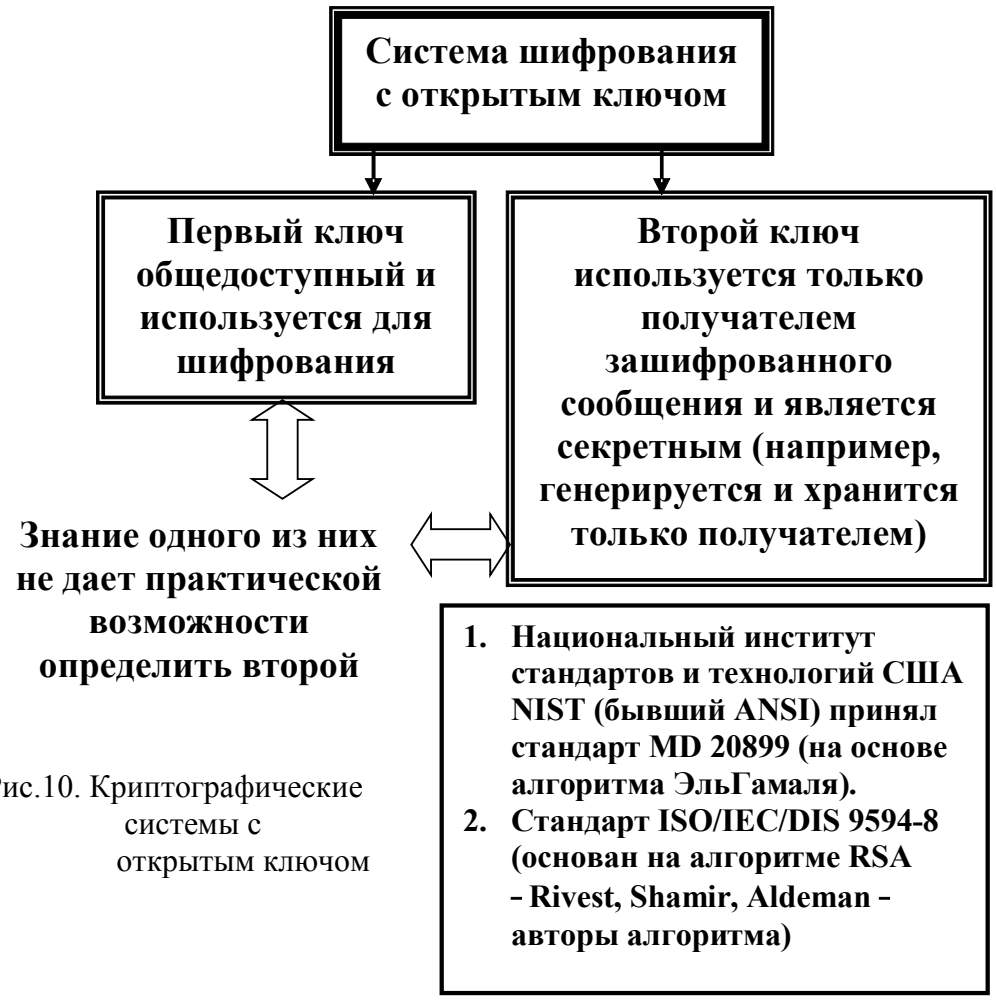


Рис.10. Криптографические системы с открытым ключом

Тема 7. СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Все многообразие существующих криптографических методов можно свести к следующим классам преобразований:

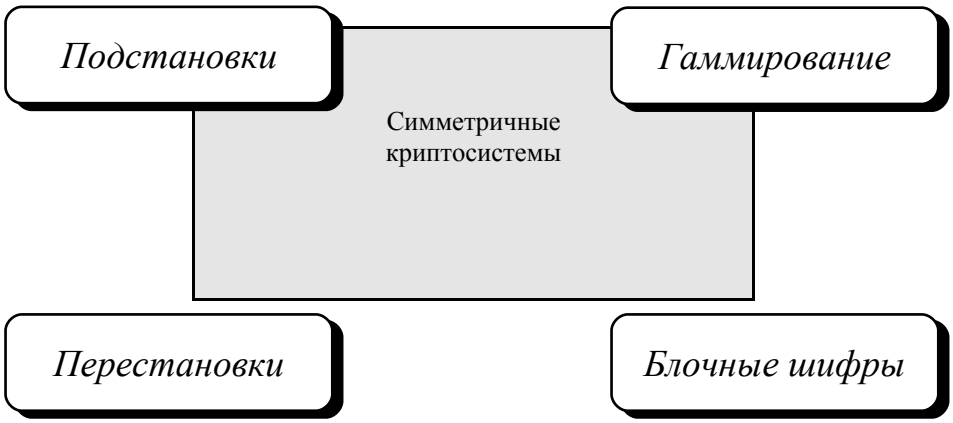


Рис.1.1.Классы преобразований симметричных криптосистем.

Многоалфавитная подстановка - наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. Для обеспечения высокой криптостойкости требуется использование больших ключей.

Перестановки - несложный метод криптографического преобразования. Используется как правило в сочетании с другими методами.

Гаммирование - этот метод заключается в наложении на исходный текст некоторой псевдослучайной последовательности, генерируемой на основе ключа.

Блочные шифры собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста. Блочные шифры на практике встречаются чаще, чем "чистые" преобразования того или иного класса в силу их более высокой криптостойкости. Российский и американский стандарты шифрования основаны именно на этом классе шифров.

Перестановкой σ набора целых чисел (0,1,...,N-1) называется его переупорядочение. Для того чтобы показать, что целое i перемещено из позиции i в позицию $\sigma(i)$, где $0 \le (i) < n$, будем использовать запись

$\sigma=(\sigma(0), \sigma(1),..., \sigma(N-1))$.

Число перестановок из (0,1,...,N-1) равно n!=1*2*...*(N-1)*N. Введем обозначение σ для взаимно-однозначного отображения (гомоморфизма) набора S={s0,s1, ...,sN-1}, состоящего из n элементов, на себя.

σ: S $\rightarrow$ S

σ: si $\rightarrow$ sσ(i), $0 \le i < n$

Будем говорить, что в этом смысле σ является перестановкой элементов S. И, наоборот, автоморфизм S соответствует перестановке целых чисел (0,1,2,.., n-1).

Криптографическим преобразованием T для алфавита Zm называется последовательность автоморфизмов: $T=\{T(n):1\le n<\infty\}$

T(n): Zm,n$\rightarrow$Zm,n, $1\le n<\infty$

Каждое T(n) является, таким образом, перестановкой n-грамм из Zm,n.

Поскольку T(i) и T(j) могут быть определены независимо при $i\neq j$, число криптографических преобразований исходного текста размерности n равно $(mn)!^{i}$. Оно возрастает непропорционально при увеличении m и n: так, при m=33 и n=2 число различных криптографических преобразований равно 1089!. Отсюда следует, что потенциально существует большое число отображений исходного текста в шифрованный.

Практическая реализация криптографических систем требует, чтобы преобразования $\{Tk: k\in K\}$ были определены алгоритмами, зависящими от относительно небольшого числа параметров (ключей).

Системы подстановок

Определение Подстановкой π на алфавите Zm называется автоморфизм Zm, при котором буквы исходного текста t замещены буквами шифрованного текста $\pi(t)$:

Zm $\rightarrow$ Zm; π: t $\rightarrow$ $\pi(t)$.

Набор всех подстановок называется симметрической группой Zm и будет в дальнейшем обозначаться как SYM(Zm).

Утверждение SYM(Zm) с операцией произведения является группой, т.е. операцией, обладающей следующими свойствами:

Замкнутость: произведение подстановок π1π2 является подстановкой:

π: t→π1(π2(t)).

Ассоциативность: результат произведения π1π2π3 не зависит от порядка расстановки скобок:

(π1π2)π3=π1(π2π3)

Существование нейтрального элемента: постановка i, определяемая как i(t)=t, 0≤t<m, является нейтральным элементом SYM(Zm) по операции умножения: iπ=πi для ∀π∈ SYM(Zm).

Существование обратного: для любой подстановки π существует единственная обратная подстановка π-1, удовлетворяющая условию

ππ-1=π-1π=i.

Число возможных подстановок в симметрической группе Zm называется порядком SYM(Zm) и равно m! .

Определение. Ключом подстановки k для Zm называется последовательность элементов симметрической группы Zm:

k=(p0,p1,...,pn-1,...), pn∈ SYM(Zm), 0≤n<∞

Подстановка, определяемая ключом k, является криптографическим преобразованием Tk, при помощи которого осуществляется преобразование n-граммы исходного текста (x0 ,x1 ,..,xn-1) в n-грамму шифрованного текста (y0 ,y1 ,...,yn-1):

yi=p(xi), 0≤i<n

где n – произвольное (n=1,2,..). Tk называется моноалфавитной подстановкой, если p неизменно при любом i, i=0,1,..., в противном случае Tk называется многоалфавитной подстановкой.

Примечание. К наиболее существенным особенностям подстановки Tk относятся следующие:

1. Исходный текст шифруется посимвольно. Шифрования n-граммы (x0 ,x1 ,..,xn-1) и ее префикса (x0 ,x1 ,..,xs-1) связаны соотношениями

Tk(x0 ,x1 ,..,xn-1)=(y0 ,y1 ,...,yn-1)

Tk(x0 ,x1 ,..,xs-1)=(y0 ,y1 ,...,ys-1)

2. Буква шифрованного текста yi является функцией только i-й компоненты ключа pi и i-й буквы исходного текста xi.

Подстановка Цезаря

Подстановка Цезаря является самым простым вариантом подстановки. Она относится к группе моноалфавитных подстановок.

Определение. Подмножество Cm={Ck: 0≤k<m} симметрической группы SYM(Zm), содержащее m подстановок

Ck: j→(j+k) (mod m), 0≤k < m,

называется подстановкой Цезаря.

Умножение коммутативно, CkCj=CjCk=Cj+k, C0 – идентичная подстановка, а обратной к Ск является Ck-1=Cm-k, где 0<k<m. Семейство подстановок Цезаря названо по имени римского императора Гая Юлия Цезаря, который поручал Марку Туллию Цицерону составлять послания с использованием 50-буквенного алфавита и подстановки C3.

Подстановка определяется по таблице замещения, содержащей пары соответствующих букв “исходный текст – шифрованный текст”. Для С3 подстановки приведены в Табл. 1. Стрелка (→) означает, что буква исходного текста (слева) шифруется при помощи С3 в букву шифрованного текста (справа).

Определение. Системой Цезаря называется моноалфавитная подстановка, преобразующая n-грамму исходного текста (x0, x1 ,..,xn-1) в n-грамму шифрованного текста (y0 ,y1 ,...,yn-1) в соответствии с правилом

yi=Ck(xi), 0≤i<n.

Например, ВЫШЛИТЕ_НОВЫЕ_УКАЗАНИЯ посредством подстановки С3 преобразуется в еюыолхиврсеюивцнгкгрлб.

А→г	Й→м	Т→х	Ы→ю
Б→д	К→н	У→ц	Ь→я
В→е	Л→о	Ф→ч	Э→_
Г→ж	М→п	Х→ш	Ю→а
Д→з	Н→р	Ц→щ	Я→б
Е→и	О→с	Ч→ъ	_→в
Ж→й	П→т	Ш→ы	
З→к	Р→у	Щ→ь	
И→л	С→ф	Ъ→э	

Таблица 1.1: Применение подстановки Цезвря.

При своей несложности система легко уязвима. Если злоумышленник имеет

1) шифрованный и соответствующий исходный текст или

2) шифрованный текст выбранного злоумышленником исходного текста,

то определение ключа и дешифрование исходного текста тривиальны.

Более эффективны обобщения подстановки Цезаря - шифр Хилла и шифр Плэйфера. Они основаны на подстановке не отдельных символов, а 2-грамм (шифр Плэйфера) или n-грамм[ii] (шифр Хилла). При более высокой криптостойкости они значительно сложнее для реализации и требуют достаточно большого количества ключевой информации.

Многоалфавитные системы. Системы одноразового использования

Слабая криптостойкость моноалфавитных подстановок преодолевается с применением подстановок многоалфавитных.

Многоалфавитная подстановка определяется ключом $\pi=(\pi 1, \pi 2, ...)$, содержащим не менее двух различных подстановок. В начале рассмотрим многоалфавитные системы подстановок с нулевым начальным смещением. Пусть {Ki: 0≤i<n} – независимые случайные переменные с одинаковым распределением вероятностей,

принимающие значения на множестве Zm

Ркл{(K0, K1, ..., Kn-1)=(k0, k1, ..., kn-1)}=(1/m)n

Система одноразового использования преобразует исходный текст

X=(X0, x1, ..., xn-1)

в шифрованный текст

Y=(Y0, y1, ..., yn-1)

при помощи подстановки Цезаря

$Yi=CKi(xi)=(Ki+Xi) \pmod m \quad i=0...n-1$ (1)

Для такой системы подстановки используют также термин “одноразовая лента” и “одноразовый блокнот”. Пространство ключей К системы одноразовой подстановки является вектором рангов (K0, K1, ..., Kn-1) и содержит mn точек.

Рассмотрим небольшой пример шифрования с бесконечным ключом. В качестве ключа примем текст

“БЕСКОНЕЧНЫЙ_КЛЮЧ....”.

Зашифруем с его помощью текст “ШИФР_НЕРАСКРЫВАЕМ”. Шифрование оформим в таблицу:

ШИФРУЕМЫЙ_ТЕКСТ	24	8	20	16	19	5	12	27	9	32	18	5	10	17	18
БЕСКОНЕЧНЫЙ_КЛЮЧ	1	5	17	10	14	13	5	23	13	27	9	32	10	11	30
ЩРДЪАТТССЦЪЫДФЫП	25	13	4	26	0	18	17	17	22	26	27	4	20	28	15

Исходный текст невозможно восстановить без ключа.

Наложение белого шума в виде бесконечного ключа на исходный текст меняет статистические характеристики языка источника. Системы одноразового использования теоретически не расшифруемы[iii], так как не содержат достаточной информации для восстановления текста.

Почему же эти системы неприменимы для обеспечения секретности при обработке информации? Ответ простой - они непрактичны, так как требуют независимого выбора значения ключа для каждой буквы исходного текста. Хотя такое требование может быть и не слишком трудным при передаче по прямому кабелю Москва - Нью-Йорк, но для информационных оно непосильно, поскольку там придется шифровать многие миллионы знаков.

Посмотрим, что получится, если ослабить требование шифровать каждую букву исходного текста отдельным значением ключа.

Системы шифрования Вижинера

Начнем с конечной последовательности ключа

$k = (k0 ,k1 ,...,kn)$,

которая называется ключом пользователя, и продлим ее до бесконечной последовательности, повторяя цепочку. Таким образом, получим рабочий ключ

$k = (k0 ,k1 ,...,kn), kj = k(j \bmod r, 0 \le j < \infty$.

Например, при $r = \infty$ и ключе пользователя 15 8 2 10 11 4 18 рабочий ключ будет периодической последовательностью:

15 8 2 10 11 4 18 15 8 2 10 11 4 18 15 8 2 10 11 4 18 ...

Определение. Подстановка Вижинера VIGk определяется как

$VIGk : (x0, x1, ..., xn-1) \rightarrow (y0, y1, ..., yn-1) = (x0+k, x1+k,. .., xn-1+k)$.

Таким образом:

1) исходный текст x делится на r фрагментов

xi = (xi , xi+r , ..., xi+r(n-1)), 0 ≤ i < r;

2) i-й фрагмент исходного текста xi шифруется при помощи подстановки Цезаря Ck :

(xi , xi+r , ..., xi+r(n-1)) → (yi , yi+r , ..., yi+r(n-1)),

Вариант системы подстановок Вижинера при m=2 называется системой Вернама (1917 г). В то время ключ k=(k0 ,k1 ,...,kк-1) записывался на бумажной ленте. Каждая буква исходного переводилась с использованием кода Бодо в пятибитовый символ. К исходному тексту Бодо добавлялся ключ (по модулю 2). Старинный телетайп фирмы AT&T со считывающим устройством Вернама и оборудованием для шифрования, использовался корпусом связи армии США.

Очень распространена плохая с точки зрения секретности практика использовать слово или фразу в качестве ключа для того, чтобы k=(k0 ,k1 ,...,kк-1) было легко запомнить. В ИС для обеспечения безопасности информации это недопустимо. Для получения ключей должны использоваться программные или аппаратные средства случайной генерации ключей.

Пример. Преобразование текста с помощью подстановки Вижинера (r=4)

Исходный текст (ИТ1):

НЕ_СЛЕДУЕТ_ВЫБИРАТЬ_НЕСЛУЧАЙНЫЙ_КЛЮЧ

Ключ: КЛЮЧ

Разобьем исходный текст на блоки по 4 символа:

НЕ_С ЛЕДУ ЕТ_В ЫБИР АТЬ_ НЕСЛ УЧАЙ НЫЙ_ КЛЮЧ

и наложим на них ключ (используя таблицу Вижинера):

Н+К=Ч, Е+Л=Р и т.д.

Получаем зашифрованный (ЗТ1) текст:

ЧРЭЗ ХРБЙ ПЭЭЩ ДМЕЖ КЭЩЦ ЧРОБ ЭБЮ_ ЧЕЖЦ ФЦЫН

Можно выдвинуть и обобщенную систему Вижинера. ЕЕ можно сформулировать не только при помощи подстановки Цезаря.

Пусть x - подмножество симметрической группы SYM(Zm).

Определение. r-многоалфавитный ключ шифрования есть r-набор π = (π 0, π1, ..., πr-1) с элементами в x.

Обобщенная система Вижинера преобразует исходный текст (x0, x1 ,..., xn-1) в шифрованный текст (y0 ,y1 ,...,yn-1) при помощи ключа π = (π0, π1, ..., πr-1) по правилу

VIGk : (x0 ,x1 ,...,xn-1) → (y0 ,y1 ,...,yn-1) = (π0(x0), π1(x1), ..., πn-1(xn-1)), где используется условие πi = πi mod r. Следует признать, что и многоалфавитные подстановки в принципе доступны криптоаналитическому исследованию. Криптостойкость многоалфавитных систем резко убывает с уменьшением длины ключа.

Тем не менее такая система как шифр Вижинера допускает несложную аппаратную или программную реализацию и при достаточно большой длине ключа может быть использован в современных ИС.

Гаммирование

Гаммирование является также широко применяемым криптографическим преобразованием. На самом деле граница между гаммированием и ис-

пользованием бесконечных ключей и шифров Вижинера, о которых речь шла выше, весьма условная.

Принцип шифрования гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы на открытые данные обратимым образом (например, используя сложение по модулю 2).

Процесс дешифрования данных сводится к повторной генерации гаммы шифра при известном ключе и наложении такой гаммы на зашифрованные данные.

Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей. По сути дела гамма шифра должна изменяться случайным образом для каждого шифруемого слова. Фактически же, если период гаммы превышает длину всего зашифрованного текста и неизвестна никакая часть исходного текста, то шифр можно раскрыть только прямым перебором (пробой на ключ). Криптостойкость в этом случае определяется размером ключа.

Метод гаммирования становится бессильным, если злоумышленнику становится известен фрагмент исходного текста и соответствующая ему шифрограмма. Простым вычитанием по модулю получается отрезок ПСП и по нему восстанавливается вся последовательность. Злоумышленники может сделать это на основе догадок о содержании исходного текста. Так, если большинство посылаемых сообщений начинается со слов “СОВ.СЕКРЕТНО”, то криптоанализ всего текста значительно облегчается. Это следует учитывать при создании реальных систем информационной безопасности.

Ниже рассматриваются наиболее распространенные методы генерации гамм, которые могут быть использованы на практике.

Шифрование с помощью аналитических преобразований

Достаточно надежное закрытие информации может быть обеспечено при использовании для шифрования некоторых аналитических преобразований. Для этого нужно использовать методы алгебры матриц , например , умножение матрицы на вектор по правилу:

$$\| a_{ij} \| b_j = c_j = \Sigma a_{ij} b_j$$

Если матрицу $\| a_{ij} \|$ использовать в качестве ключа , а вместо компонента вектора b_j подставить символы текста , то компоненты вектора c_j будут представлять собой символы зашифрованного текста.

Приведем пример , взяв в качестве ключа квадратную матрицу третьего порядка

$$\begin{vmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{vmatrix}$$

Заменим буквы алфавита цифрами, соответствующими порядковому номеру в алфавите. Тогда отрывку текста ВАТАЛА соответствует последовательность номеров 3,0,19,0,12,0. По принятому алгоритму шифрования выполним необходимые действия:

$$\begin{vmatrix}14 & 8 & 3\\ 8 & 5 & 2\\ 3 & 2 & 1\end{vmatrix} * \begin{vmatrix}3\\ 0\\ 19\end{vmatrix} = \begin{vmatrix}99\\ 62\\ 28\end{vmatrix} \quad ; \quad \begin{vmatrix}14 & 8 & 3\\ 8 & 5 & 2\\ 3 & 2 & 1\end{vmatrix} * \begin{vmatrix}0\\ 12\\ 0\end{vmatrix} = \begin{vmatrix}96\\ 60\\ 24\end{vmatrix}$$

При этом зашифрованый текст будет иметь вид:99,62,28,96,60,24.

Расшифрование осуществляетсяс использованием того же правила умножения матрицы на вектор, только в качестве основы берется матрица, обратная той, с помощью которой осуществляется закрытие, а в качестве вектора-самножителя – соответствующие колличество символов закрытого текста; тогда значениями вектора-результата будут цифровые эквиваленты знаков открытого текста. Обратной к данной называется матрица, полущающая из так называемой присоединенной матрицы делением всех ее элементов на определитель данной матрицы. В свою очередь присоединенной называется матрица, составленная из алгеброических дополнений A ,к элементам данной матрицы, которые вычисляются по формуле:

Aij = (-1)^i+j Dij ,

где Dij – определитель матрицы, получаемый вычеркиванием i-й ее строки и j-го столбца. Определителем же как известно, называется алгеброическая сумма n! членов (для определения n-ого порядка), составленная следующим образом: членами служат всевозможные произведения n элементов матрицы, взятых по одному в каждой строке и в каждом столбце, причем член суммы берется со знаком "+", если его индексы составлят подставку, и со знаком "-" - в противоположном случае. Для матрицы третьего порядка, например, определитель вычисляется по следующей формуле:

D=a11a22a33+a12a23a31+a13a21a32-a11a23a32-a12a21a33-a13a22a31.

Тогда процесс раскрытия выглядит так:

$$\begin{vmatrix}1 & -2 & 1\\ -2 & 5 & -4\\ 1 & -4 & 6\end{vmatrix} * \begin{vmatrix}99\\ 62\\ 28\end{vmatrix} = \begin{vmatrix}1*99-2*62+1*28\\ -2*99+5*62-4*28\\ 1*99-4*62+6*28\end{vmatrix} = \begin{vmatrix}3\\ 0\\ 19\end{vmatrix}$$

$$\begin{vmatrix}1 & -2 & 1\\ 2 & 5 & -4\\ 1 & -4 & 6\end{vmatrix} * \begin{vmatrix}96\\ 60\\ 24\end{vmatrix} = \begin{vmatrix}1*96-2*60+1*24\\ -2*96+5*60-4*24\\ 1*96-4*60+6*24\end{vmatrix} = \begin{vmatrix}0\\ 12\\ 0\end{vmatrix}$$

Таким образом, получили следующую последовательность знаков раскрытого текста:3,0,19,0,12,0, что соответствует исходному тексту. Этот метод шифрования является формальным, что позволяет легко реализовать его программными средствами.

Криптосистемы на основе эллиптических уравнений

Эллиптические кривые - математический объект, который может определен над любым полем (конечным, действительным, рациональным или комплексным). В криптографии обычно используются конечные поля. Эллиптическая кривая есть множество точек (x,y), удовлетворяющее следующему уравнению:

y2 = x3 + ax + b,

а также бесконечно удаленная точка. Для точек на кривой довольно легко вводится операция сложения, которая играет ту же роль, что и операция умножения в криптосистемах RSA и Эль-Гамаля.

В реальных криптосистемах на базе эллиптических уравнений используется уравнение

$y2 = x3 + ax + b \bmod p$,

где p - простое.

Проблема дискретного логарифма на эллиптической кривой состоит в следующем: дана точка G на эллиптической кривой порядка r (количество точек на кривой) и другая точка Y на этой же кривой. Нужно найти единственную точку x такую, что Y = xG, то есть Y есть x-я степень G.

Тема 8. ЦИФРОВАЯ ПОДПИСЬ

10 января 2002 года Президентом был подписан очень важный закон "Об электронной цифровой подписи"(13 декабря 2001 г), развивающий и конкретизирующий приведенные выше положения закона "Об информации...". Его роль поясняется в статье I.

1. Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись и электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

2. Действие настоящего Федерального закона распространяется на отношения, возникающие при свершении гражданско-правовых сделок и в других предусмотренных Законодательством РФ случаях. Действие настоящего Федерального закона не распространяется на отношения возникающие при использовании иных аналогов собственноручной подписи. Закон вводит следующие основные понятия

Электронный документ - документ, в котором информация представлена в электронно-цифровой форме.

Электронная цифровая подпись - реквизит электронного документа, предназначенный для зашиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытою ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Средства электронной цифровой подписи - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном

документе с использованием скрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Сертификат средств электронной цифровой подписи — документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Закрытый ключ электронной цифровой подписи — уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи

Открытый ключ электронной цифровой подписи — уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Сертификат ключа подписи - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Подтверждение подлинности электронной цифровой подписи в электронном документе — положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Пользователь сертификата ключа подписи - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификат ключа подписи.

Информационная система общего пользования — информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Корпоративная информационная система — информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Пересказать такие определения своими словами невозможно…..

Согласно Закону, электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Закон определяет сведения, которые должен содержать сертификат ключа подписи:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима запись об этом вносится удостоверяющим центром в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
- наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

Криптография с открытым ключом прекрасно подходит для замены обычной подписи электронной. Действующие в России системы передачи данных в большинство своем имеют один значительный недостаток – не дают возможности проверки подлинности и авторства пересылаемых документов (невозможность заключение юридически признаваемых сделок и пересылка юридически подтверждаемых документов). Исключением является ранее отмеченная плата “Криптон”. В ней и ряда других систем цифровая подпись сообщения формируется с помощью секретного ключа, которая может быть очень длинной. По этой причине шифруется только сделанная по тексту сообщения контрольная сумма (называется имитоприставкой). Например, в одной из таких систем длина ключа состоит из 128 бит и это обеспечивает качественный “отпечаток пальцев”, (вероятность подделки меньше 10^{-38}). Однако восстановить оригинальное сообщение по этому цифровому ключу невозможно.

Проблема авторства документа может быть решена лишь с использованием электронной цифровой подписи – средства, позволяющего на основе криптографических методов надежно установить авторство и подлинность документа (см. рис. 11). Здесь вместо обычной связи между печатью или рукописной подписью и листом бумаги выступает сложная математическая зависимость между документом, секретным и общедоступном ключами, а также

цифровой подписью. Невозможность подделки электронной цифровой подписи опирается именно на большой объем необходимых математических вычислений.

Имеются примеры функций криптографического преобразования, для которых сложность подделки цифровой подписи при отсутствии секретной информации заверяющего такова, что самая мощная из существующих ЭВМ не сможет осуществить необходимые вычисления и за десятки лет.

Системы шифрования с открытым ключом тоже не решают все проблемы, которые стоят перед криптографами. Например, нечестному пользователю ничего не стоит под своей настоящей подписью поставить фальшивую дату (для финансовых документов это может быть катастрофой). Поэтому цифровая подпись с датой должна заверяться третьим лицом (как нотариус).

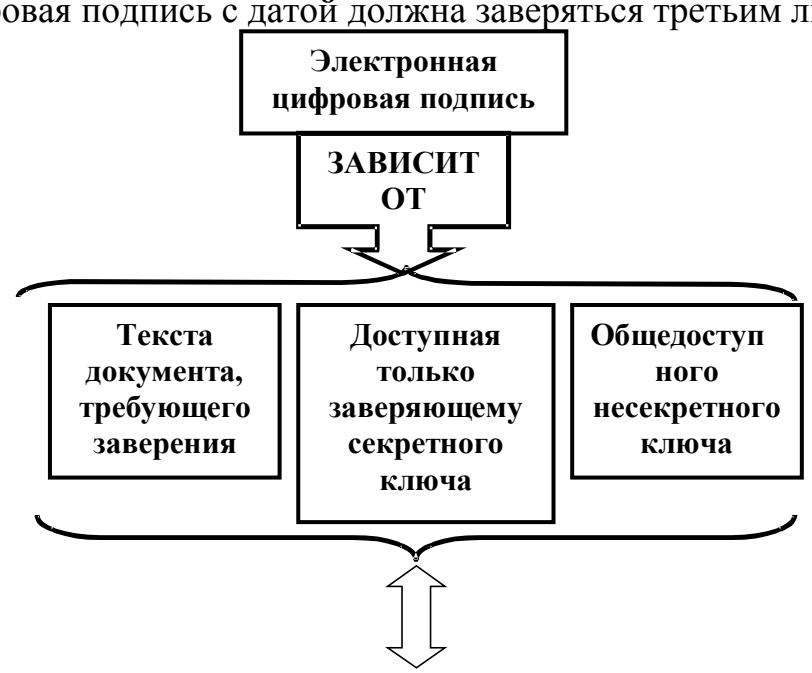


Рис. 11. Составляющие электронной цифровой подписи

4. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Лабораторные работы имеют различный уровень сложности и на их выполнение требуется различное количество часов. Каждая предполагает самостоятельную работу студентов по освоению лекций и теоретического материала, вынесенного на самостоятельное изучение. Текущий контроль знаний осуществляется путем опроса студентов перед началом лабораторного занятия по вопросам, перечень которых приведен в каждой лабораторной работе.

Лабораторная работа 1. ОЦЕНОЧНЫЙ РАСЧЕТ ЗАЩИЩЕННОСТИ ПОМЕЩЕНИЯ ОТ УТЕЧКИ РЕЧЕВЫХ СООБЩЕНИЙ ПО АКУСТИЧЕСКОМУ КАНАЛУ

Циркуляция в помещении акустических колебаний, вызванных как значимыми для информационного обмена потоками речевых сообщений между их прямыми носителями (людьми), так и незначительными, но информативными потоками акустических колебаний (клавиатура ПЭВМ, пишущая машинка или телетайп, принтер и т.п.), при недостаточной звукоизоляции ограждающих конструкций, а также при наличии косвенных носителей информации (акустоэлектрических, акустовибрационных и акустооптических преобразователей) в этом помещении может привести к распространению сообщений по **обобщенному** акустическому каналу, средой передачи в котором могут являться:

в акустическом канале - окружающее воздушное пространство;

в акустоэлектрическом канале - провода, отходящие от различных электромеханических преобразователей, находящихся в помещении, за пределы этого помещения;

в акустовибрационном канале - стены и перегородки, перекрытия, оконные рамы, дверные коробки, трубопроводы, короба вентиляции;

- в акустооптическом канале - оптоволоконный кабель.

Акустический канал возникает из-за образования звуковых волн сжатия, создаваемых голосовым аппаратом человека, и распространения их в воздушной среде, а также проникновения через несущие стены зданий, окна, двери, вентиляционные воздуховоды сквозь поры, щели и т.п.

При произнесении звуков речи через речевой тракт, представляющий собой сложный акустический фильтр с рядом резонаторов, создаваемых полостями рта, носа и носоглотки, проходит либо тональный импульсный сигнал (звонкие звуки), либо шумовой (глухие звуки), либо тот и другой вместе. Вследствие этого равномерный тональный или шумовой спектр превращается в спектр с рядом максимумов, называемых формантами, и минимумов, называемых антиформантами. Так как наиболее информативными являются глухие согласные, то при действии шумов разборчивость речи снижается, в первую очередь из-за маскировки глухих звуков. Ухо человека обладает свойствами дискретного восприятия по частотному и динамическому диапазонам.

Слуховое ощущение пропорционально логарифму раздражающей силы:

$$\mathbf{E}_{\text{дБ}}=10\boldsymbol{lg}(\mathbf{I}/\mathbf{I}_{\text{п.с}}), \qquad (1)$$

где $\mathbf{I}_{п.с}$ - раздражающая сила на пороге слышимости.

Величину **E** называют уровнем ощущения, причем $\mathbf{E} = \mathbf{L}_1 - \mathbf{L}_{п.с}$, где $\mathbf{L}_1 = 10\boldsymbol{lg}\mathbf{I} + 120$ - уровень интенсивности звука **I**, Вт/м^2. Уровень ощущения, представляет собой уровень над порогом слышимости, т.е. относительный уровень.

Так как уровень ощущения неточно характеризует субъективное ощущение, в акустике применяется понятие "уровень громкости" звука (или шума), под которым понимается уровень в децибелах равногромкого с ним чистого тона 1000 Гц.

В соответствии с кривыми равной громкости, при уровне 30-40 фон (уровень громкости в дБ на частоте 1000 Гц) в диапазоне частот 250...500 Гц происходит уменьшение громкости примерно на 6 дБ, поэтому при приеме элементов речи техническими средствами, это снижение можно компенсировать частотной коррекцией, что невозможно осуществить при приеме речи специально подготовленными людьми - артикулянтами.

Восприятие речи в значительной степени зависит от уровня акустических шумов, которые могут распространяться и как акустические сигналы и как помехи. Последние подразделяются на три вида: белый шум (имеет одинаковую спектральную плотность во всем частотном диапазоне), розовый (имеет тенденцию спада на 3 дБ/окт в сторону высоких частот) и речевой шум - шум, создаваемый одновременным разговором нескольких человек.

Обычно при расчетах рассматриваются стационарные шумы, однако в течение длительного периода времени (день - ночь, рабочие дни - выходные) шумы могут носить нестационарный характер, т.е. изменяться во времени. Маскирующие свойства шумов проявляются тем сильнее, чем больше их превышение над полезным сигналом во всей полосе частот речевого диапазона. Наибольший маскирующий эффект имеют широкополосные помехи с "гладким" спектром, но удовлетворительная разборчивость речи может быть достигнута даже в том случае, если уровень речи будет на несколько децибел ниже уровня шума.

Узкополосные помехи даже высокого уровня не могут обеспечить требуемой степени зашумления речи, так как они, как правило, имеют периодический характер, что позволяет частично их компенсировать с помощью различных фильтров.

Для определения максимально допустимого уровня шума в помещениях, в соответствии с санитарными нормами, применяются предельные спектры (ПС). Число при ПС означает уровень шума в октавной полосе со среднегеометрической частотой 1000 Гц. Так как санитарные нормы ограничивают максимальное значение уровня шума для различных типов помещений, то предельные спектры можно использовать для расчета разборчивости речи в конкретных условиях.

Уровни интенсивности речи в октавных полосах и некоторые значения предельных спектров шумов приводятся в табл. 1. Значения уровней шумов, измеренные на частоте 1000 Гц в различных местах, приводятся в табл. 2.

Разборчивостью называют относительное или процентное количество принятых специально тренированными слушателями (артикулянтами) эле-

ментов речи из общего количества переданных по тракту. Так как в качестве элементов речи применяют звуки, слоги, слова и фразы, то имеет место **звуковая, слоговая, словесная и фразовая** разборчивость. Все они при испытании одной и той же системы будут выражаться разными численными величинами, так как процент правильных оценок для предвиденного сообщения всегда выше, чем для непредвиденного, степень же предвидения при прослушивании фразы выше, чем при прослушивании отдельных слов или слогов.

Однако все виды разборчивости связаны друг с другом однозначными функциональными зависимостями, представляемыми обычно в виде кривых или таблиц.

Разборчивость представляет собой статистическую характеристику речи, принимаемой на фоне шумов, и описывается вероятностными характеристиками. Она может характеризовать качество канала только в среднем значении, допуская флуктуации в ту или иную сторону.

Объективные измерительные оценки разборчивости речи могут производиться с помощью вычисления разборчивости формант. По формантной разборчивости **А**ф определяют слоговую **S**, словесную **W**, фразовую разборчивость и понятность речи. Зависимость между формантной **А**ф (суммарной вероятностью приема формант), слоговой S и словесной **W** разборчивостью речи приведена в табл.3.

Форманты звуков речи заполняют весь частотный диапазон 150...7000 Гц. Этот частотный диапазон делят на 20 полос равной разборчивости. Вероятность появления формант в каждой полосе равной разборчивости равна 0,05. При прослушивании речи в условиях шумов разборчивость получается меньшей, чем в их отсутствие. Коэффициент ***w***, определяющий это уменьшение, называют ***коэффициентом восприятия, или коэффициентом разборчивости***, т.е. в каждой полосе равной разборчивости вероятность приема формант $\Delta\mathbf{A} = 0{,}05\,\boldsymbol{w}$. Коэффициент разборчивости ***w*** определяется уровнем ощущения формант $\mathbf{E}_{ф} = \mathbf{B}_{р.} - \mathbf{B}_{ш.}$, где $\mathbf{B}_{р.}$ - средний спектральный уровень речи; $\mathbf{B}_{ш.}$ - спектральный уровень шумов.

Для практики применение полос равной разборчивости неудобно, так как получающиеся частотные полосы нестандартны. Для каждой полосы равной разборчивости коэффициент разборчивости ***w*** в общем случае будет разный, поэтому в акустических измерениях используются октавные или третьоктавные частотные полосы. Значения коэффициентов разборчивости речи ***w***, соответствующие определенным уровням ощущения формант **Е**ф, приведены в табл. 4.

Градации понятности речи и соответствующие им значения слоговой (**S**) и словесной (**W**) разборчивости, измеренные артикулянтами и дополненные значениями формантной **А**ф разборчивости (суммарной вероятностью приема формант), взятой из табл. 3, приведены в табл. 5. Учитывая, что восприятие человеком формант обладает свойством аддитивности, т.е. каждый участок речевого диапазона вносит свой вклад в общую разборчивость речи, можно рассчитать вклады октавных полос для формантной разборчивости. На основании данных о вкладах октавного анализа для русской речи можно

определить выражение для формантной разборчивости **А**ф.русск. для русской речи:

А ф.русск.= 0,05*(1,34***w*1** + 2,5 ***w*2** + 4,24***w*3** +5,88 ***w*4**+5***w*5**+1,04***w*6**), (2)

где ***w***i - коэффициенты разборчивости речи на средних октавных частотах (250, 500, 1000, 2000, 4000, 6000).

От качественного приема каждой частотной полосы зависит суммарная разборчивость. Минимальная формантная разборчивость Аф, при которой еще возможно понимание смысла речевого сообщения (суммарная вероятность приема формант), равна 15%, что соответствует 25% слоговой и 75% словесной разборчивости (см. табл. 5).

Учитывая сказанное, для минимальной формантной разборчивости можно записать: **А**ф.русск.мин = 0,05 (1,34***w*1 + 2,5***w*2 + 4,24***w*3 + 5,88***w*4 + 5w5 + 1,04***w*6) = 0,15.

Рассчитаем ***w***i на частоте 1000 Гц, так как на этой частоте обычно приводятся значения коэффициента звукоизоляции ограждающих конструкций.

Суммарной вероятности приема формант **А**ф.русск.мин = 0,15 соответствует 100% всего частотного диапазона, а участку, который вносит свой вклад в разборчивость в размере 21,2% (на частоте 1000 Гц), соответствует W_{1000} = W3 = 0,05x4,24x0,15 /100 = 3,15/100 = 0,0315. Согласно табл. 4 для W = 0,03 находим Еф = Вр. – Вш. = - 9 дБ. Так как ухо человека обладает свойствами дискретного восприятия по частотному и динамическому диапазонам, то для того, чтобы речь была вообще неразборчива, возьмем предыдущее значение W = 0,02, для которого Еф. = Вр. – Вш. = -10 дБ на частоте 1000 Гц.

Проведя аналогичные действия для остальных пяти октавных полос, а также повторив их для удовлетворительной, хорошей и отличной суммарных вероятностей приема формант для всех шести октавных полос, сведем полученные результаты в табл. 6.

На разборчивость речевых сообщений оказывает влияние эффект реверберации, характеризуемый временем уменьшения уровня звукового давления в помещении на 60 дБ после выключения источника. Этот эффект проявляется в наложении речевых отрезков друг на друга за счет переотражения сигнала от поверхностей конструкций, поэтому если помещение имеет звукопоглощающие поверхности, то время реверберации незначительно, однако в больших гулких помещениях реверберация может существенно исказить речь. Время реверберации менее 0,85 сек. незаметно для слуха. Для большинства кабинетов и помещений с мебелью их объемы и акустическая отделка позволяют не учитывать временные искажения, так как время реверберации в них не превышает 0,6 сек.

При падении звуковых волн с интенсивностью $\mathbf{I}_{пад.}$ на какую-либо перегородку больших размеров в сравнении с длиной волны интенсивность звука с другой стороны перегородки $\mathbf{I}_{пр}$ в условиях отсутствия отражения звука в пространстве за перегородкой будет определяться только звукопроводностью перегородки. Коэффициент звукопроводности $\alpha_{пр} = \mathbf{I}_{пр} / \mathbf{I}_{пад} = \rho^2_{пр} / \rho^2_{пад}$ или в

логарифмических единицах (звукоизоляция перегородки) $\mathbf{Q}_{пер} = \mathbf{L}_{пад} - \mathbf{L}_{пр} = 20\boldsymbol{lg}(\rho_{пад}/\rho_{пр})$, где $\mathbf{L}_{пад}$ и $\mathbf{L}_{пр}$ - уровни звукового давления с внутренней и внешней сторон перегородки, $\rho_{пад}$ и $\rho_{пр}$ – поверхностная плотность материала перегородки с внутренней и внешней сторон. Коэффициент звукоизоляции стен $\mathbf{Q}_{пер}$ с различной поверхностной плотностью ρ в децибелах (с учетом только мембранного переноса) для частот 500...1000 Гц может быть определен по формулам:

$$\mathbf{Q}_{пер}, \text{ дБ} = 12{,}5\boldsymbol{lg}\rho + 14 \quad (3)$$

для стен с $\rho < 200$ кг/м^2;

$$\mathbf{Q}_{пер}, \text{ дБ} = 14{,}5\boldsymbol{lg}\rho + 15 \quad (4)$$

для стен с $\rho > 200$ кг/м^2;

$$\mathbf{Q}_{пер}, \text{ дБ} = 14\boldsymbol{lg}\,(\rho_1\rho_1) + 20\,\boldsymbol{lg}\delta - 13 \quad (5)$$

для двойных жестких перегородок с воздушной прослойкой между ними с поверхностной плотностью ρ = 30...100 кг/м^2; где $\rho 1$ и $\rho 1$ - поверхностная плотность первой и второй перегородки, δ - толщина воздушного слоя между ними.

Значения $\mathbf{Q}_{пер}$ в формулах 3 - 5 приводятся для частот 500...1000 Гц; для частот 50...250 Гц звукоизоляция будет на 6 дБ меньше, а для частот, равных 4000 Гц и более на 6 дБ больше. Некоторые значения $\mathbf{Q}_{пер}$ приводятся в табл. 7.

Изолирующие свойства перегородки с дверью или окном можно рассчитать по следующей формуле:

$$\mathbf{Q}_{пер} = \mathbf{Q}1 - 10\boldsymbol{lg}[1 + (\mathbf{S}_o/(\mathbf{S}_1 + \mathbf{S}_o))*(10^{0{,}1(\mathbf{Q}1-\mathbf{Q}o)} - 1)], \quad (6)$$

где $\mathbf{Q}_{пер}$ - величина звукоизоляции неоднородной перегородки;

$\mathbf{Q}_1$ - величина звукоизоляции глухой части перегородки (без учета окна или двери);

$\mathbf{Q}_o$ - величина звукоизоляции двери или окна;

$\mathbf{S}_1$ - площадь глухой части стены;

$\mathbf{S}_o$ - площадь двери или окна.

При прохождении через различные строительные конструкции и материалы сигналы ослабевают в зависимости от толщины и поверхностной плотности материала. Уровень акустического сигнала за ограждающей конструкцией (звукоизолирующей перегородкой) $\mathbf{L}_2$ можно определить из следующего выражения:

$$\mathbf{L}_2 = \mathbf{L}_1 + 10\boldsymbol{lg}(\mathbf{S}/\mathbf{A}) - \mathbf{Q}_{пер}, \quad (7)$$

где: $\mathbf{L}_2$ - уровень речевого сигнала за звукоизолирующей перегородкой;

$\mathbf{L}_1$- уровень речевого сигнала в контролируемом помещении;

S - площадь звукоизолирующей перегородки, разделяющей помещения;

A - эквивалентная площадь звукопоглощения, м^2;

$\mathbf{Q}_{пер}$ - коэффициент звукоизоляции различных конструкций для частот 500...1000 Гц.

Для ориентировочной оценки звукоизоляции меблированных помещений величина $10\boldsymbol{lg}(\mathbf{S}/\mathbf{A})$, характеризующая реверберационные

свойства помещения, может быть принята равной нулю. С учетом этого, а также предполагая, что в качестве приемника речевых сообщений используется техническое средство, которое может иметь на низких частотах подъем усиления на 6 дБ, выражение для определения $\mathbf{L}_2$ примет вид:

$$\mathbf{L}_2 = \mathbf{L}_1 + 6 - \mathbf{Q}_{пер}. \quad (8)$$

Это выражение в дальнейшем будем применять для расчетов уровня речевого сигнала за звукоизолирующей перегородкой.

Таблица 1.

Уровни интенсивности речи в октавных полосах и предельные спектры шумов

Номер октавы	Средняя частота, *f*р	Уровни речи и предельные спектры шумов, дБ								
		речь	ПС-20	ПС-25	ПС-30	ПС-35	**ПС-40**	ПС-45	ПС-50	ПС-55
1	250	67,9	31	35	40	45	49	54	59	63
2	500	66,9	24	29	34	39	44	49	54	58
3	1000	61,5	20	25	30	35	40	45	50	55
4	2000	57,0	17	22	27	32	37	42	47	52
5	4000	53,0	14	20	25	30	35	40	44	50
6	6000	48,5	13	18	23	28	33	38	43	49
Суммарные уровни, дБ		71	32,3	36,6	41,6	47	51	60	61	65

ПС-25 - кабинет при одном работающем;
ПС-30 - библиотека;
ПС-35 - комната для сна и отдыха;
ПС-45 - кабинет для умственной работы без собственных шумов;
ПС-50 - кабинет для речевой и телефонной связи;
ПС-55 - кабинет для конторского труда и цеховой администрации

Таблица 2.

Уровни шумов, измеренные на частоте 1000 Гц

Источник шума и место его измерения	Уровень шума, дБ (f = 1000Гц)
акустические шумы вне помещений:	
тихий сад	20
тихая улица (без движения транспорта)	30-35
обычный средний шум на улице	55-60
шумная улица без трамвайного движения	60-75
трамвай на расстоянии 10-20 м	80-85

троллейбус на расстоянии 5 м	77

Продолжение таблицы 2.

грузовой автомобиль в городе на расстоянии 10-20 м	60-75
легковой автомобиль в городе на расстоянии 10-20 м	50-65
электропоезд на эстакаде на расстоянии 6 м	90
акустические шумы в помещениях:	
обычное учреждение, жилое помещение	40
шепот на расстоянии 1 м	20-25
спокойный разговор 3 человек в комнате средних размеров	45-50
громкая музыка по радио	80
Разговор на расстоянии 1 м: обычный	55-60
громкий	65-70
громкий разговор по телефону	55
шумное собрание	65-70
коридоры	35-40
бухгалтерия без посетителей	30-35
комната шумная	40-50
комната тихая	25-30
кабинет при одном работающем	20-25

Таблица 3.

Зависимость между формантной (Аф), слоговой (S)
и словесной (W) разборчивостью

Аф, отн. ед.	S**, %**	**W**, %	**А**ф, отн. ед.	S**, %**	**W**, %
0,05	5,0	30,0	0,55	84,0	98,5
0,10	15,0	63,0	0,60	87,0	98,8
0,15	26,0	76,0	0,65	90,0	99,0
0,20	36,0	85,0	0,70	92,5	99,2
0,25	46,0	90,0	0,75	95,2	99,4
0,30	54,0	93,0	0,80	96,5	99,6
0,35	62,5	94,5	0,85	98,0	99,7
0,40	69,0	96,0	0,90	99,0	99,8
0,45	75,0	97,0	0,95	99,5	99,9
0,50	80,0	98,0	1,00	100,0	100,0

Таблица 4.

Значения коэффициентов разборчивости ***w***,
соответствующие определенным уровням ощущения формант **Е**ф

Еф, дБ	***w***, отн. ед.	**Е**ф, дБ	***w***, отн. ед.	**Е**ф, дБ	***w***, отн. ед.	**Е**ф, дБ	***w***, отн. ед.
Еф < 15 ***w*** = 0		-8	0,040	9	0,50	26	0,960
		-7	0,050	12	0,60	27	0,970
		-6	0,060	15	0,70	28	0,980
		-5	0,075	18	0,80	29	0,985
-15	0,002	-4	0,095	19	0,83	30	0,990
-14	0,005	-3	0,110	20	0,86	33	0,995
-13	0,007	-2	0,140	21	0,88	36	1,000
-12	0,010	-1	0,17	22	0,900	**Е**ф > 36 ***w*** = 1	
-11	0,015	0	0,20	23	0,915		
-10	0,020	3	0,30	24	0,930		
-9	0,030	6	0,40	25	0,945		

Таблица 5.

Градации понятности речи и соответствующие им значения формантной (**А**ф), слоговой (**S**) и словесной (**W**) разборчивости

Понятность	**Разбочивость, %**		
	форматная (**А**ф)	слоговая (**S**)	словестная (**W**)
Предельно допустимая	15-22	25-40	75-87
Удовлетворительная	22-31	40-56	87-93
Хорошая	31-50	56-80	93-98
Отличная	50 и выше	80 и выше	98 и выше

Таблица 6.

Разборчивость речи и уровни ощущения формант в октавных полосах

Аф.русск. = 0,05*(1,34***w***1 +2,5***w***2 +4,24***w***3 + 5,88 ***w***4 +5***w***5 +1,04***w***6)							
		Средняя частота октавных полос, Гц					
		250	500	1000	2000	4 000	6000
		Вклад частот в разбочивость формант, %					
		6,7	12,5	21,2	29,4	25	5,2
Понятность речи	**Суммарная** разборчивость формант Аф.русск., %	Разборчивость речи в конкретной октавной полосе частот, ***w***i					

Продолжение таблицы 6

		Уровень ощущения формант Еф. = Вр. – Вш. в конкретной октавной полосе, дБ					
Смысл непонятен	< 15	**0 <-12**	**0,015 -11**	**0,02 -10**	**0,03 -9**	**0,03 -9**	**0 <-12**
Предельно допустимая	15 – 22	**0,01 -12**	**0,02 -10**	**0,03 -9**	**0,04 -8**	**0,04 -8**	**0,007 <-12**
Удовлетворительная	22 – 31	**0,015 -11**	**0,03 -9**	**0,04 -8**	**0,06 -6**	**0,05 -7**	**0,011 -12**
Хорошая	31 – 50	**0,02 -10**	**0,04 -8**	**0,06 -6**	**0,09 -4**	**0,077 -5**	**0,016 -11**
Отличная	>= 50	**0,03 -9**	**0,06 -6**	**0,11 -3**	**0,147 -2**	**0,125 -2**	**0,026 -10**

Таблица 7.

Значения коэффициентов звукоизоляции материалов и ограждающих конструкций

	Материал или конструкция	Толщина, мм	Поверхностная плотность, кг/м^2	**Q**пер, дБ
1.Стены и перегородки				
Стена из кирпичной кладки без штукатурки (из красного кирпича):				
1.1.	в 0,5 кирпича	120,0	204,0	48,0
1.2.	в 1 кирпич	250,0	425,0	53,0
1.3.	в 1,5 кирпича	380,0	646,0	56,0
1.4.	в 2 кирпича	520,0	884,0	58,0
1.5.	в 2,5 кирпича	640,0	1088,0	59,0
1.6.	Виброкирпичная панель, не оштукатуренная	140,0	240,0	49,5
1.7.	То же	160,0	280,0	50,4
1.8.	Стена из пустотелого кирпича	380,0	-	51,0
1.9.	То же	510,0	-	54,0
1.10.	Стена из железобетона	100,0	240,0	49,0
1.11.	То же	140,0	340,0	51,0
1.12.	То же	160,0	400,0	52,0
1.13.	То же	180,0	430,0	53,0
1.14.	То же	200,0	500,0	54,0
1.15.	То же	300,0	750,0	56,6
1.16.	То же	800,0	2000,0	62,8
1.17.	Гипсобетонная (гипсолитовая) плита	80,0	115,0	39,7
1.18.	То же	95,0	135,0	40,6
1.19.	Газобетонная плита	240,0	270,0	50,25

Продолжение таблицы 7

1.20.	Керамзитобетонная плита	80,0	100,0	39,0
1.21.	То же	100,0	150,0	41,2
1.22.	То же	120,0	195,0	42,6
1.23.	Шлакоблоки, оштукатуренные с двух сторон	220,0	360,0	52,0
	Шлакогибсовые стенные плиты:			
1.24.	2х5 см	130,0	120,0	40,0
1.25.	2х6 см	170,0	150,0	42,0
	Пемзобетонные стенные плиты:			
1.26.	2х6 см	150,0	135,0	40,0
1.27.	2х8,5 см	200,0	185,0	43,0
1.28.	Стены из пемзобетона	140,0	150,0	42,0
1.29.	То же	230,0	250,0	50,0
1.30.	Стена из шлакобетона	140,0	150,0	42,0
1.31.	То же	250,0	400,0	52,7
1.32.	То же из пустотелых пемзобетонных блоков	190,0	190,0	43,0
1.33.	То же	290,0	270,0	50,0
1.34.	Древесно-стружечная плита	20,0	12,0	27,4
1.35.	Перегородка одинарная из досок толщиной 2 см, оштукатуренная с обеих сторон и оклеенная обоями	60,0	70,0	37,0
1.36.	Перегородка одинарная из досок толщиной 2,5 см, оштукатуренная с обеих сторон по войлоку	70,0	76,0	39,0
1.37.	Перегородка двойная из брусков 10 см, обшитых с двух сторон досками толщиной 2,5 см и отштукатуренная с двух сторон	180,0	95,0	45,0
1.38.	То же с отштукатуркой по войлоку	190,0	96,0	47,0
1.39.	Перегородка двойная из фанерных листов толщиной 3 мм с промежутком 2,5 см, заполненным шлаковатой	30,0	8,0	26,0
1.40.	То же с промежутком 5 см	55,0	12,0	29,0
1.41.	То же с промежутком 6,5 см	70,0	14,0	34,0

Продолжение таблицы 7

1.42.	Гипсовые пустотелые камни толщиной 1 см с двумя стенками толщиной по 1,5 см и промежутком 8 см с засыпкой шлаком	110,0	117,0	41,0
2. Окна				
2.1.	Одинарное остекление без уплотнительных прокладок	3,0	-	22,0
2.2.	Тоже	4,0	-	26,0
2.3.	Тоже	6,0	-	26,0
2.4.	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала (нар.- внутр.)	3,0/3,0	-	32,0
2.5.	То же со звукопоглощающим материалом	3,0/3,0	-	42,0
2.6.	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала	3,0/3,0	-	38,0
2.7.	То же со звукопоглощающим материалом	3,0/3,0	-	43,0
2.8.	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала	4,0/4,0	-	38,0
2.9.	То же со звукопоглощающим материалом	4,0/4,0	-	41,0
2.10.	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала	4,0/4,0	-	41,0
2.11.	Двойное остекление, расстояние между стеклами 57 см, без звукопоглощающего материала	6,0/3,0	-	35,0
2.12.	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала	6,0/3,0	-	37,0
2.13.	Двойное остекление, расстояние между стеклами 38 мм, без звукопоглощающего материала	6,0/6,0	-	40,0
2.14.	То же, 190 мм	6,0/6,0	-	45,0
2.15.	То же, 400 мм	6,0/6,0	-	48,0

Продолжение таблицы 7

3. Двери				
	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см:			
3.1.	без уплотняющих прокладок	-	-	18,0
3.2.	с уплотняющими прокладками	-	-	23,0
3.3.	То же, с обвязкой толщиной 2,5 см и филенкой из 3 мм фанеры без уплотняющих прокладок	-	-	10,0
3.4.	То же, оклеенная фанерой размером 90х200 см ,без уплотняющих прокладок	-	-	22,0
	Глухая щитовая дверь толщиной 40 мм, облицованная с двух сторон фанерой толщиной 4 мм:			
3.5.	без уплотняющих прокладок	-	-	24,0
3.6.	с уплотняющими прокладками	-	-	32,0
	Щитовая дверь из твердых древесно-волокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненная стекловатой:			
3.7.	без уплотняющих прокладок	-	-	30,0
3.8.	с уплотняющими прокладками	-	-	33,0
	То же, заполненная минеральным войлоком:			
3.9.	без уплотняющих прокладок	-	-	28,0
3.10.	с уплотняющими прокладками	-	-	32,0
3.11.	Тяжелая дубовая дверь размером 90х210 см, плотно пригнанная	-	-	25,0
3.12.	Металлическая дверь (герметичная)	-	-	30,0

Пример расчетов по определению возможности утечки речевых сообщений

Рассмотрим возможность утечки речевых сообщений из исследуемого кабинета (рис. 1).

Исходные данные расчетов:

а) смежная комната: предельный спектр шумов - **ПС**-35 (табл. 1); перегородка одинарная из досок (п. 136 табл. 7);

б) внутренний двор здания: предельный спектр шумов - **ПС**-45 (табл. 1); стена из кирпичной кладки (п. 1.5 табл. 7); окно (п. 2.6 табл. 7) занимает 40% стены;

в) коридор: предельный спектр шумов - **ПС**-40 (табл. 1); стена из кирпичной кладки (п.1.1 табл. 7); дверь (п. 3.1 табл. 7) занимает 20% стены;

г) уровень интенсивности речи в октавных полосах берется из табл. 1.

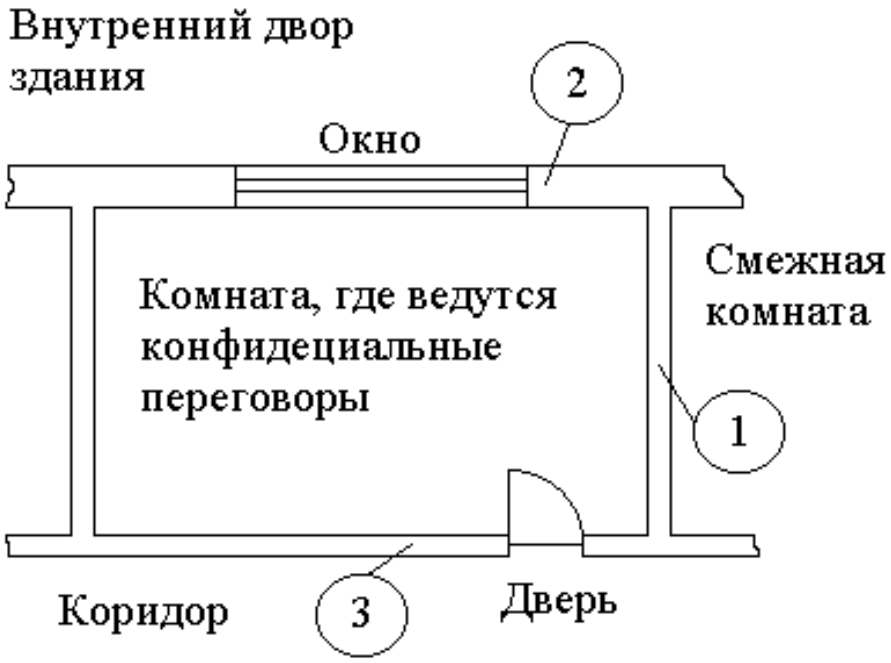


Рис. 1. Схема исследуемого кабинета

Порядок расчета.

1. Смежная комната.

По формуле (8) определяем: $\mathbf{L}_2 = \mathbf{L}_1 + 6 - \mathbf{Q}_{пер}$,

где $\mathbf{L}_2$ - уровень речевого сигнала за звукоизолирующей перегородкой;

$\mathbf{L}_1$ - уровень речевого сигнала в контролируемом помещении.

Значение $\mathbf{L}_1$ в октавных полосах будем определять, исходя из суммарного уровня речи 71 дБ (табл. 1). Значение $\mathbf{Q}_{пер}$ берем в табл. 1.

Номер октавы	Ср. частота, $f_р$	Уровни речи Речь, **L**1	Коэф. звукоизоляции с учетом повышения на частотах 4000, 6000 и понижения на частоте 250 на 6 дБ $\mathbf{Q}_{пер}$	**L**1 + 6 - $\mathbf{Q}_{пер}$, дБ	**L**2 = **L**р, дБ
1.	250	67,9	39-6	67,9 + 6 - (39 - 6)	40,9
2.	500	66,9	39	66,9 + 6 - 39	33,9
3.	1000	61,5	39	61,5 + 6 -39	28,5
4.	2000	57,0	39	57,0 + 6 - 39	24,0
5.	4000	53,0	39+6	53,0 + 6 - (39 + 6)	14,0
6.	6000	48,5	39+6	48,5 + 6 - (39 + 6)	9,5

Уровень ощущения формант $\mathbf{E}_ф$ определяется из выражения:

Eф= **L**р – **L**ш.

Номер октавы	Ср. частота, $f_р$	**L**2 = **L**р, дБ	Предельные спектры шумов ПС-35, **L**ш, дБ	**E**ф= **L**р – **L**ш, дБ	Значения коэф. разборчивости w_i по табл. 3
1.	250	40,9	45	-4,1	0,095
2.	500	33,9	39	-5,1	0,075

3.	1000	28,5	35	-6,5	0,06
4.	2000	24,0	32	-8	0,04
5.	4000	14,0	30	-16	0
6.	6000	9,5	28	-18,5	0

По формуле (2) находим суммарную разборчивость формант:

А ф.русск.= 0,05*(1,34***w***1 + 2,5 ***w***2 + 4,24***w***3 +5,88 ***w***4+5***w***5+1,04***w***6) =

= 0,05*(1,34x0,095 + 2,5x0,075 + 4,24x0,06 + 5,88x0,004) =

= 0,04 или (4%)

Выводы: расчетная суммарная разборчивость формант **А**ф.русск. <15%, в соответствии с табл. 6 смысл разговора в смежной комнате будет непонятен.

2. Внешняя стена

По формуле (6) определяем величину звукоизоляции неоднородной перегородки, которыми являются внешняя стена и окно:

Qпер = **Q**1-10***lg***[1+(**S**o/(**S**1 + **S**o))*($10^{0,1(\mathbf{Q}1-\mathbf{Q}o)}$-1)],

где **Q**1 = 59 дБ;

Qo = 38 дБ;

(**S**o/(**S**1 + **S**o)) = 0,4.

Qпер = 59-10***lg***[1+0,4*($10^{0,1(59-38)}$-1)] = 42 Дб.

Уменьшение звукоизоляции стены с окном составило 17 дБ.

Дальнейшие вычисления проводим аналогично с п.1.

Номер октавы	Ср. частота, ***f***р	Уровни речи Речь, **L**1	Коэф. звукоизоляции с учетом повышения на частотах 4000, 6000 и понижения на частоте 250 на 6 дБ **Q**пер	**L**1 + 6 - **Q**пер, дБ	**L**2 = **L**р, дБ
1.	250	67,9	42-6	67,9 + 6 - (42 - 6)	37,9
2.	500	66,9	42	66,9 + 6 - 42	30,9
3.	1000	61,5	42	61,5 + 6 -42	25,5
4.	2000	57,0	42	57,0 + 6 - 42	21,0
5.	4000	53,0	42+6	53,0 + 6 - (42 + 6)	11,0
6.	6000	48,5	42+6	48,5 + 6 - (42 + 6)	6,5

Уровень ощущения формант **Е**ф определяется из выражения:

Еф= **L**р – **L**ш.

Номер октавы	Ср. частота, ***f***р	**L**2 = **L**р, дБ	Предельные спектры шумов ПС-45, **L**ш, дБ	**Е**ф= **L**р – **L**ш, дБ	Значения коэф. разборчивости ***w***i по табл. 3
1.	250	37,9	54	-16,1	0
2.	500	30,9	49	-18,1	0
3.	1000	25,5	45	-19,5	0
4.	2000	21,0	42	-21,0	0
5.	4000	11,0	40	-29,0	0
6.	6000	6,5	38	-31,5	0

По формуле (2) находим суммарную разборчивость формант

А ф.русск.= 0 (0%).

Выводы: расчетная суммарная разборчивость формант Аф.русск. < 15%, в соответствии с табл. 6 смысл разговора за окном не будет понятен.

3. Коридор

По формуле (6) определяем величину звукоизоляции неоднородной перегородки, которыми являются внутренняя стена и дверь:

Qпер = **Q**1-10***lg***[1+(**S**o/(**S**1 + **S**o))*($10^{0,1(Q1-Qo)}$-1)],

где **Q**1 = 48 дБ;

Qo = 18 дБ;

(**S**o/(**S**1 + **S**o)) = 0,2.

Qпер = 59-10***lg***[1+0,2*($10^{0,1(48-18)}$-1)] = 25 дБ

Уменьшение звукоизоляции стены с дверью составило 23 дБ.

Дальнейшие вычисления проводим аналогично с п.1.

№ октавы	Ср. частота, ***f***р	Уровни речи Речь, **L**1	Коэф. звукоизоляции с учетом повышения на частотах 4000, 6000 и понижения на частоте 250 на 6 дБ **Q**пер	**L**1 + 6 - **Q**пер, дБ	**L**2 = **L**р, дБ
1.	250	67,9	25-6	67,9 + 6 - (25 - 6)	54,9
2.	500	66,9	25	66,9 + 6 - 25	47,9
3.	1000	61,5	25	61,5 + 6 - 25	42,5
4.	2000	57,0	25	57,0 + 6 - 25	38
5.	4000	53,0	25+6	53,0 + 6 - (25 + 6)	28
6.	6000	48,5	25+6	48,5 + 6 - (25 + 6)	23,5

Уровень ощущения формант **E**ф определяется из выражения:

Eф= **L**р – **L**ш.

№ октавы	Ср. частота, ***f***р	**L**2 = **L**р, дБ	Предельные спектры шумов ПС-40, **L**ш, дБ	**E**ф= **L**р – **L**ш, дБ	Значения коэффициентов разборчивости ***w***i по табл. 3
1.	250	54,9	49	5,9	0,4
2.	500	47,9	44	3,9	0,35
3.	1000	42,5	40	2,5	0,3
4.	2000	38	37	1	0,25
5.	4000	28	35	-7	0,05
6.	6000	23,5	33	-9,5	0,03

По формуле (2) находим суммарную разборчивость формант

А ф.русск.= 0,05*(1,34***w***1 + 2,5 ***w***2 + 4,24***w***3 +5,88 ***w***4+5***w***5+1,04***w***6) =

= 0,05*(1,34x0,4 + 2,5x0,35 + 4,24x0,3 + 5,88x0,25 +

+ 5,0x0,05 + 1,04x0,03) = 0,22 (22%).

Выводы: расчетная суммарная разборчивость формант Аф.русск. =

22%. В соответствии с табл. 6 смысл разговора за дверью будет понятен, слышимость удовлетворительная. Необходимо обеспечить звуковую изоляцию стены и двери.

Задание.

В соответствии со схемой (рис. 1) рассчитать суммарную разборчивость формант в смежном помещении, коридоре и за наружной стеной. Сделать выводы о возможности или невозможности утечки звуковой информации.

Уровни интенсивности речи в октавных полосах берутся из табл. 1, для всех вариантов они одинаковы.

Номер вариан-та	1. Смежное помещение	2. Наружная стена	3. Коридор
1.	Стена (табл. 7, п. 1.1) **ПС**-25 (табл. 1)	Стена (табл. 7, п. 1.2) Окно (табл. 7, п. 2.1) **S**o = 40% **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.1) Дверь (табл. 7, п. 3.1) **S**o = 20% **ПС**-25 (табл. 1)
2.	Стена (табл. 7, п. 1.6) **ПС**-30 (табл. 1)	Стена (табл. 7, п. 1.3) Окно (табл. 7, п. 2.2) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7, п. 1.6) Дверь (табл. 7, п. 3.2) **S**o = 30% **ПС**-30 (табл. 1)
3.	Стена (табл. 7, п. 1.10) **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.4) Окно (табл. 7, п. 2.3) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7, п. 1.10) Дверь (табл. 7, п. 3.3) **S**o = 20% **ПС**-35 (табл. 1)
4.	Стена (табл. 7, п. 1.17) **ПС**-25 (табл. 1)	Стена (табл. 7, п. 1.5) Окно (табл. 7, п. 2.4) **S**o = 40% **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.17) Дверь (табл. 7, п. 3.4) **S**o = 30% **ПС**-25 (табл. 1)
5.	Стена (табл. 7, п. 1.18) **ПС**-30 (табл. 1)	Стена (табл. 7, п. 1.7) Окно (табл. 7, п. 2.5) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7, п. 1.18) Дверь (табл. 7, п. 3.5) **S**o = 20% **ПС**-30 (табл. 1)
6.	Стена (табл. 7, п. 1.20) **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.8) Окно (табл. 7, п. 2.6) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7, п. 1.20) Дверь (табл. 7, п. 3.6) **S**o = 30% **ПС**-35 (табл. 1)
7.	Стена (табл. 7, п. 1.21) **ПС**-25 (табл. 1)	Стена (табл. 7, п. 1.9) Окно (табл. 7, п. 2.7) **S**o = 40% **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.21) Дверь (табл. 7, п. 3.7) **S**o = 20% **ПС**-25 (табл. 1)
8.	Стена (табл. 7, п. 1.22) **ПС**-30 (табл. 1);	Стена (табл. 7, п. 1.13) Окно (табл. 7, п. 2.8) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7, п. 1.22) Дверь (табл. 7, п. 3.8) **S**o = 30% **ПС**-30 (табл. 1)

Номер вариан-та	1. Смежное помещение	2. Наружная стена	3. Коридор
9.	Стена (табл. 7, п. 1.24) **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.14) Окно (табл. 7, п. 2.9) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7, п. 1.24) Дверь (табл. 7, п. 3.9) **S**o = 20% **ПС**-35 (табл. 1)
10.	Стена (табл. 7, п. 1.25) **ПС**-25 (табл. 1)	Стена (табл. 7, п. 1.15) Окно (табл. 7, п. 2.10) **S**o = 40% **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.25) Дверь (табл. 7, п. 3.10) **S**o = 30% **ПС**-25 (табл. 1)
11.	Стена (табл. 7, п. 1.26) **ПС**-30 (табл. 1)	Стена (табл. 7, п. 1.16) Окно (табл. 7, п. 2.11) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7, п. 1.26) Дверь (табл. 7, п. 3.11) **S**o = 20% **ПС**-30 (табл. 1)
12.	Стена (табл. 7, п. 1.30) **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.19) Окно (табл. 7, п. 2.12) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7, п. 1.30) Дверь (табл. 7, п. 3.1) **S**o = 30% **ПС**-35 (табл. 1)
13.	Стена (табл. 7, п. 1.34) **ПС**-25 (табл. 1)	Стена (табл. 7, п. 1.27) Окно (табл. 7, п. 2.13) **S**o = 40% **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.34) Дверь (табл. 7, п. 3.2) **S**o = 20% **ПС**-25 (табл. 1)
14.	Стена (табл. 7, п. 1.35) **ПС**-30 (табл. 1)	Стена (табл. 7, п. 1.31) Окно (табл. 7, п. 2.14) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7, п. 1.35) Дверь (табл. 7, п. 3.3) **S**o = 30% **ПС**-30 (табл. 1)
15.	Стена (табл. 7, п. 1.36) **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.23) Окно (табл. 7, п. 2.15) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7, п. 1.36) Дверь (табл. 7, п. 3.4) **S**o = 20% **ПС**-35 (табл. 1)
16.	Стена (табл. 7, п. 1.37) **ПС**-25 (табл. 1)	Стена (табл. 7, п. 1.32) Окно (табл. 7, п. 2.1) **S**o = 40% **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.37) Дверь (табл. 7, п. 3.5) **S**o = 30% **ПС**-25 (табл. 1)
17.	Стена (табл. 7, п. 1.38) **ПС**-30 (табл. 1)	Стена (табл. 7, п. 1.3) Окно (табл. 7, п. 2.2) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7, п. 1.38) Дверь (табл. 7, п. 3.6) **S**o = 20% **ПС**-30 (табл. 1)
18.	Стена (табл. 7, п. 1.39) **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.32) Окно (табл. 7, п. 2.3) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7, п. 1.39) Дверь (табл. 7, п. 3.7) **S**o = 30% **ПС**-35 (табл. 1)
19.	Стена (табл. 7, п. 1.40) **ПС**-25 (табл. 1)	Стена (табл. 7, п. 1.23) Окно (табл. 7, п. 2.4) **S**o = 40%	Стена (табл. 7, п. 1.40) Дверь (табл. 7, п. 3.8) **S**o = 20%

Номер варианта	1. Смежное помещение	2. Наружная стена	3. Коридор
		ПС-35 (табл. 1)	**ПС**-25 (табл. 1)
20.	Стена (табл. 7, п. 1.41) **ПС**-30 (табл. 1)	Стена (табл. 7, п. 1.31) Окно (табл. 7, п. 2.5) **S**o = 50% **ПС**-40 (табл. 1)	Стена (табл. 7, п. 1.41) Дверь (табл. 7, п. 3.9) **S**o = 30% **ПС**-30 (табл. 1)
21.	Стена (табл. 7, п. 1.42) **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.19) Окно (табл. 7, п. 2.6) **S**o = 60% **ПС**-45 (табл. 1)	Стена (табл. 7, п. 1.42) Дверь (табл. 7, п. 3.10) **S**o = 20% **ПС**-35 (табл. 1)

Лабораторная работа 2. ОЦЕНОЧНЫЙ РАСЧЕТ ЗАЩИЩЕННОСТИ ПОМЕЩЕНИЙ УТЕЧКИ ИНФОРМАЦИИ ПО ЭЛЕКТРОМАГНИТНОМУ КАНАЛУ

Обобщенный электромагнитный канал (канал побочных электромагнитных излучений и наводок - ПЭМИН) состоит из каналов утечки, причинами возникновения которых являются:

излучения в окружающее пространство (в дальней зоне) электромагнитных полей технических средств (ТС) и соединяющих их линий связи (например, электромагнитное поле монитора и других устройств ПЭВМ);

излучение в окружающее пространство (в ближней зоне) электрической составляющей электромагнитного поля ТС (например, электрическое поле, излучаемое клавиатурой);

излучение в окружающее пространство (в ближней зоне) магнитной составляющей электромагнитного поля ТС (например, магнитное поле усилителя звуковой частоты);

паразитные наводки на отходящие и проходящие вблизи от ТС провода и кабели, на расположенные рядом внешние технические средства связи, взаимные наводки между линиями связи, обусловленные:

а) непосредственными электрической и магнитной паразитными связями в ближней зоне (например, наводки на провода электропитания, заземления (зануления), выходящие из ПЭВМ линии связи - сетевой адаптер, модем);

б) емкостной и индуктивной паразитными связями по посторонним проводам, проходящим рядом с ПЭВМ (например: проходящие вблизи ПЭВМ телефонные провода и стоящих рядом телефонные аппараты, провода и кабели от других устройств и т.п.);

в) паразитной связью через электромагнитное поле излучения в дальней зоне (например, наводки на провода, кабели ТС, расположенные на значительном удалении от ПЭВМ, но проходящие в непосредственной близости от линий передачи данных (телефонных проводов и кабелей ЛВС) и проводов электропитания, выходящих из ПЭВМ);

г) паразитными связями через общее полное сопротивление (например, наводки на провода электропитания, осуществляются через элементы фильтров питания).

Наличие сигналов, несущих конфидециальные сообщения, на границе и за пределами контролируемой зоны (КЗ) создает условия для утечки сообщений за счет перехвата этих сигналов злоумышленниками.

Совокупность источника информативного сигнала, среды распространения этого сигнала и приемника перехвата злоумышленника представляет собой “канал утечки” сообщений, эффективность которого определяется следующими факторами:

уровень информативного сигнала от источника;

ослабление и искажение сигнала в среде его распространения;

технические характеристики приемного устройства, используемого злоумышленником.

Чем ближе приемник сигнала к источнику, тем эффективнее работает канал утечки. Системным показателем качества канала утечки является отношение сигнал/помеха на входе приемника перехвата, которое определяется соотношениями параметров всех элементов канала утечки.

При организации защитных мероприятий исходят из того, что приемное устройство для перехвата информативных сигналов реализует потенциальную помехоустойчивость и может быть размещено в любом месте за пределами контролируемой зоны, вплоть до ее границы. При этом считается, что наблюдение и перехват могут осуществляться непрерывно в течение времени любой продолжительности.

Определяющий вид помех в канале утечки сообщений - аддитивные помехи, характеризующиеся тем, что смесь сигнала ***s(t)*** и помехи ***n(t)*** на входе приемника представляет собой их сумму: ***x(t) = s(t) + n(t).***

Примером аддитивных помех являются:

атмосферные помехи, обусловленные электрическими процессами в атмосфере, прежде всего грозовыми разрядами;

космические помехи, вызванные радиоизлучением Солнца и других небесных тел;

внутренние шумы радиоприемника, обусловленные хаотическим движением носителей заряда в самом приемнике;

индустриальные помехи, обусловленные работой электрических устройств и агрегатов;

помехи от посторонних радиостанций.

Атмосферные помехи - тот вид помех, который всегда присутствует в окружающем пространстве, поэтому при определении дальности распространения сообщений по каналу ПЭМИН необходимо учитывать не только естественное затухание сигнала, но и искажения, вносимые этими помехами. Остальные виды помех в данной лабораторной работе не учитываются.

Для расчета среднеквадратического значения напряженности поля $\mathbf{E}_a$ атмосферных помех используется следующая формула:

$$\mathbf{E}_a = 10\mathbf{lg}(\boldsymbol{T}_a/\boldsymbol{T}_o) - 95{,}5 + 20\mathbf{lg}\boldsymbol{f} + 10\mathbf{lg}\boldsymbol{f}_{экв}, \text{ дБ}, \qquad (1)$$

где $\boldsymbol{f}$ - частота (Мгц);

$f_{экв}$ -ширина полосы пропускания приемника (Гц);

T_a - эквивалентная шумовая температура, характеризующая интенсивность помех;

$T_o = 273^oK$.

Ширина полосы пропускания приемника $f_{экв}$ в диапазоне частот выше 30 МГц должна быть не менее 40 кГц, что соответствует характеристикам целого ряда устройств, предназначенных для осуществления съема и анализа информации с ПЭВМ.

В соответствии с выражением (1) и значениях $T_a = 293^oK$, $f_{экв}$=40 Мгц расчитаем среднеквадратическую напряженность поля E_a:

на частоте 100 Мгц - E_a = -9,2 дБ (0,346 мкВ/м);

на частоте 500 Мгц - E_a = 4,8 дБ (1,738 мкВ/м);

на частоте 1000 Мгц - E_a = 10,8 дБ (3,467 мкВ/м).

Электромагнитное поле, создаваемое промышленными ВЧ-установками, затухает со средним коэффициентом:

$$k_з = 1 / r^n, \qquad (2)$$

где **r** - расстояние от источника;

n = 1,3 - 2,8 (**n** = 1,3 - для открытых сельских районов; **n** = 2,8 - для интенсивно застроенных городских районов).

Напряженность электромагнитного поля, создаваемого ПЭВМ, сертифицированной по ЭМС в соответствии с требованиями CISPR, не должна превышать:

в диапазоне 30 - 230 МГц - 630,5 мкВ/м;

в диапазоне 230 - 1000 МГц - 1412,5 мкВ/м.

Электромагнитное поле также затухает с коэффициентом $k_{экр}$ при распространении через ограждающие конструкции. Значения коэффициентов экранирования некоторых ограждающих конструкций приведены в табл. 1.

Таблица 1

Значения коэффициентов экранирования некоторых ограждающих конструкций на частотах 100, 500 и 1000 МГц

Номер п/п	Тип здания	Экранирование (дБ) (коэффициент экранирования $k_{экр}$) на частотах:		
		100 Мгц	500 МГц	1000 МГц
	Деревянное здание с толщиной стен 20 см:			
1.	окно без решетки	5-7 (1,8-2,2)	7-9 (2,2-2,8)	9-11 (2,8-3,5)
2.	окно закрыто решеткой с ячейкой 5 см	6-8 (2,0-2,5)	10-12 (3,2-4,0)	12-14 (4,0-5,0)
	Кирпичное здание с толщиной кирпичной стены 1,5 кирпича:			
3.	окно без решетки	13-15 (4,5-5,6)	15-17 (5,6-7,0)	16-19 (6,3-8,9)
4.	окно закрыто решеткой с ячейкой 5 см	17-19 (7,0-8,9)	20-22 (10,0-12,6)	22-25 (12,6-17,8)

	Железобетонные здания с ячейкой арматуры 15х15 см и толщиной 160 мм:			
5.	окно без решетки	20-25 (10,0-17,8)	18-19 (8,0-8,9)	15-17 (5,6-7,0)
6.	окно закрыто решеткой с ячейкой 5 см	28-32 (25,1-39,8)	23-27 (14,1-22,4)	20-25 (10,0-17,8)
Примечание: оконный проем составляет не более 30% от площади стены.				

Напряженность электромагнитного поля **E** на границе контролируемой зоны вычисляется по следующей формуле:

$$\mathbf{E}_{кз} = \mathbf{E}^* \mathbf{k}_з * \mathbf{k}_{экр} \text{ (мкВ/м)}, \quad (3)$$

где **E** - напряженность электромагнитного поля непосредственно у ПЭВМ;

$\mathbf{k}_з$ - коэффициент затухания (2);

$\mathbf{k}_{экр}$ - коэффициент экранирования (табл. 1).

Для обнаружения сигналов известной формы в шумах наибольшее распространение получил критерий максимума отношения пикового значения сигнала ***s(t)*** к среднеквадратическому значению σ шума на выходе оптимального фильтра, которое определяется отношением полной энергии входного сигнала к спектральной плотности мощности входного белого шума (атмосферные помехи):

$$\Delta = \frac{S(t)_{вых}}{\sigma_{вых}} = \sqrt{\frac{2Q_{вх}}{N_{0вх}}}, \quad (4)$$

где **Q** - полная энергия сигнала на входе приемника перехвата;

$\mathbf{N}_0/2$ - спектральная плотность мощности белого шума (атмосферной помехи) на входе приемника;

s(t) - пиковое значение сигнала на выходе фильтра приемника;

σ - среднеквадратическое значение помехи на выходе фильтра приемника.

Для практического применения формулы (4) необходимо определить максимальное значение Δ, при котором исключается определение злоумышленником содержания (смысла) перехваченного сообщения, т.е. определить смысловой критерий безопасности сообщений.

Было показано, что значение Δ не должно превышать:

$\Delta \le 1$ (для важных информации); (5)

$\Delta \le 0{,}7$ (для весьма важной информации). (6)

При приеме методом накопления, отношение сигнал/помеха Δ_Σ на входе решающего устройства ($2\mathbf{Q}/\mathbf{N}_O$) возрастает в **n** (количество повторений) раз по сравнению с отношением сигнал/помеха на входе приемника при однократном отсчете, т.е.:

$$\Delta_\Sigma = \sqrt{\frac{2Q}{N_0}} = \Delta\sqrt{n} \le 1. \quad (7)$$

Чтобы это соотношение выполнялось, Δ_Σ должно быть в $\sqrt{n}$ раз меньше Δ, определенной без учета повторений.

$$\Delta_{\Sigma} \leq \frac{\Delta}{\sqrt{n}}. \qquad (8)$$

Величину **n** можно установить из следующих соображений. При просмотре изображения на экране дисплея в течение t сек. изображение появляется $f_{\text{разв}}\mathbf{t}/2$ раз при чересстрочной кадровой развертке. С учетом сказанного, выражение (8) принимает следующий вид:

$$\Delta_{\Sigma} = \Delta \sqrt{\frac{2}{f_{\text{раз в}}\mathrm{t}}}. \qquad (9)$$

В соответствии с формулой (9) при частоте кадровой развертки 85 Гц и просмотре изображения в течение 15 сек. отношение сигнал/шум **Δ** на границе контролируемой зоны должно быть не более 0,04. Время, равное 15 сек. выбрано из тех соображений, что устройства, осуществляющие накопление сигналов на фоне помех, эффективно работают только в течение первых 10-15 сек. после перехвата сообщений.

Приведем пример расчета защищенности помещения от утечки информации по электромагнитному каналу. В качестве источника электромагнитного излучения возьмем ПЭВМ, расположенную на некотором удалении от контролируемой зоны (рис.1).

Пример расчета.

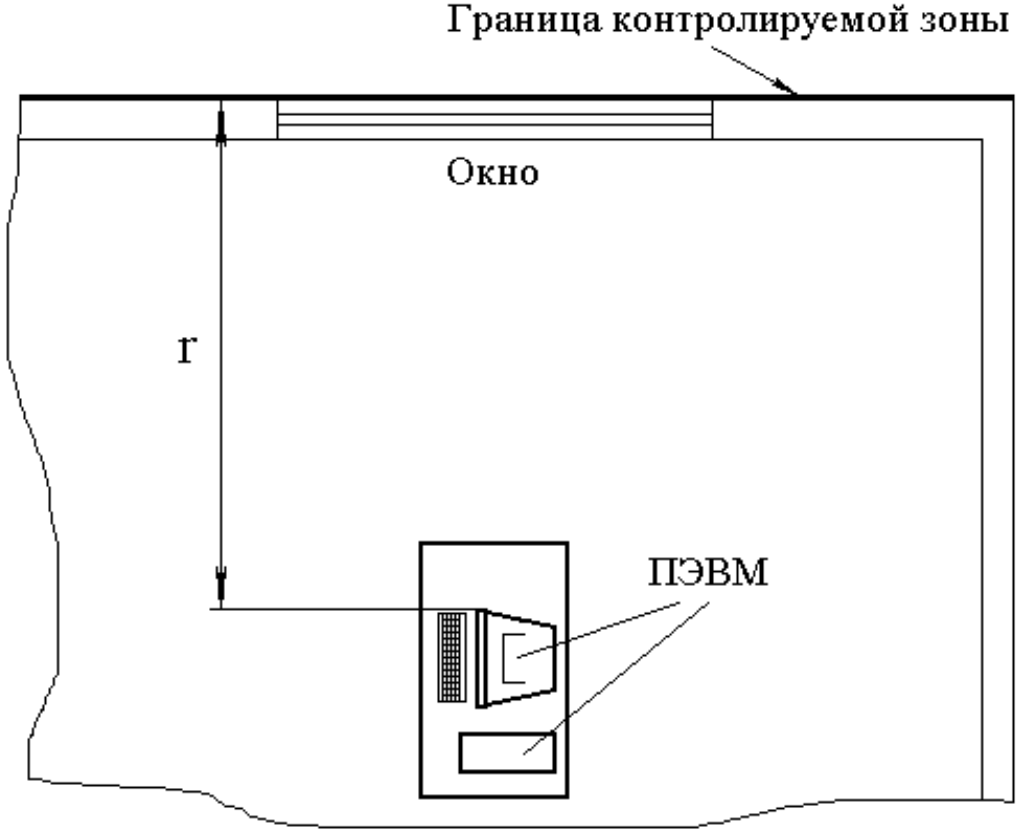


Рис. 2. Схема помещения для проведения расчетов

Таблица 2

Значения напряженности электромагнитного поля **E**, создаваемого ПЭВМ

Номер п/п	Значения электромагнитного поля **E** (мкВ/м) на частотах		
	100 МГц	500 МГц	1000 МГц
1.	630	1400	1400
2.	610	1370	1390
3.	620	1420	1400
4.	610	1360	1400
5.	600	1360	1390
6.	630	1410	1400

Исходные данные.

В помещении расположена ПЭВМ (рис.1), на которой обрабатываются конфидециальные данные. Расстояни от ПЭВМ до контролируемой зоны составляет r = 15 м. Граница контролируемой зоны проходит по периметру железобетонной стены толщиной 160 мм, в стене имеется оконный проем, не превыщающий 30% площади стены. Окно закрыто металлической решеткой с ячейкой 5 см (табл. 1, п. 6). Значения напряженности электромагнитного поля **E**, создаваемого ПЭВМ на частотах 100 МГц, 500МГц и 1000 МГц, берем из табл. 2, п. 6. При определении коэффициента затухания принимаем **n**=1,4. В качестве кретерия защищенности помещения от утечки информации на границе контролируемой зоны отношение сигнал / шум принимаем равным $\Delta \leq 1$.

Результаты расчета сводим в таблицу:

Ход вычислений	Данные, полученные из таблиц или в результате расчетов, на частотах		
	100 МГц	500 МГц	1000 МГц
Из табл. 2, п. 6 выбираем значения электромагнитного поля **E**, создаваемого ПЭВМ, мкВ/м	610	1370	1390
Определяем коэффициент затухания по формуле $\mathbf{k}_з = 1 / \mathbf{r}^n$, **r** = 15, **n** = 1,4	0,0226		
Выбираем из табл. 2, п. 6 максимальные значения коэффициента экранирования $\mathbf{k}_{экр}$	39,8	22,4	17,8
Определяем напряженность электромагнитного поля на границе контролируемой зоны по формуле (2) $\mathbf{E}_{кз} = \mathbf{E}^* \mathbf{k}_з * \mathbf{k}_{экр}$, мкВ/м	0,346	1,38	1,76
Определяем среднеквадратическое значение напряженности поля $\mathbf{E}_а$ атмосферных помех по формуле (1), принимая $\mathbf{T}_а = 293^oK$, $f_{экв}$=40 МГц	0,346	1,738	3,467
Определяем отношение сигнал/шум на границе контролируемой зоны по фор-	0,999≈1	0,79	0,51

муле $\Delta = E_{кз} / E_a$			

Расчеты показали, что на всех частотах значение $\Delta \leq 1$. Следовательно, расстояние до границы контролируемой зоны достаточно для обеспечения безопасности сообщений, излучаемых в окружающее пространство ПЭВМ. Дополнительных мер по обеспечению защиты помещения от утечки информации не требуется.

Задание

1. В соответствии со схемой (рис. 1) произвести расчеты защищенности помещения от утечки информации по электромагнитному каналу.

Среднеквадратические значения напряженности поля E_a атмосферных помех не расчитывать, считать одинаковыми для всех вариантов и равными:

	100 МГц	500 МГц	1000 МГц
E_a , мкВ/м (T_a=293°K, fэкв=40 Мгц)	0,346	1,738	3,467

Варианты:

Номер варианта	$k_з = 1 / r^n$		$k_{экр}$ Таб. 1, пункт	E Таб. 2, пункт	Δ
	r	n			
1.	15	1,3	1	1	1
2.	20	1,4	2	2	1
3.	15	1,5	3	3	1
4.	20	1,6	4	4	1
5.	15	1,7	5	5	1
6.	20	1,8	6	6	1
7.	15	1,4	1	2	1
8.	20	1,5	2	3	1
9.	15	1,6	3	4	1
10.	20	1,7	4	5	1
11.	15	1,8	5	6	1
12.	20	1,3	6	1	0,7
13.	15	1,5	1	3	0,7
14.	20	1,6	2	4	0,7
15.	15	1,7	3	5	0,7
16.	20	1,8	4	6	0,7
17.	15	1,3	5	1	0,7
18.	20	1,4	6	2	0,7
19.	15	1,6	1	4	0,7
20.	20	1,7	2	5	0,7
21.	15	1,8	3	6	0,7

2. По заданным значениям Δ рассчитать **r** для частот 100, 500 и 1000 МГц.

Лабораторная работа 3. ИЗУЧЕНИЕ ТРАДИЦИОННЫХ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ.ШИФРЫ ПЕРЕСТАНОВКИ

1. Основные понятия и определения

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования – расшифровки.

В соответствии со стандартом ГОСТ 28147-89 под шифром понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом криптографического преобразования.

Ключ - это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Основной характеристикой шифра является *криптостойкость,* которая определяет его стойкость к раскрытию методами криптоанализа. Обычно эта характеристика определяется интервалом времени, необходимым для раскрытия *шифра.*

К шифрам, используемым для криптографической защиты информации, предъявляется ряд требований:

достаточная криптостойкость (надежность закрытия данных);

простота процедур шифрования и расшифровки;

незначительная избыточность информации за счет шифрования;

нечувствительность к небольшим ошибкам шифрования и др.

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста. При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

Шифры перестановки самые простые и, вероятно, самые древние шифры.

Шифр перестановки "скитала"

Известно, что в V в. до н. э. правители Спарты, наиболее воинственного из древнегреческих государств, имели хорошо отработанную систему секретной военной связи и шифровали свои послания с помощью **скитала**. - первого простейшего криптографического устройства, реализующего метод простой перестановки.

Шифрование выполнялось следующим образом. На стержень цилиндрической формы, который назывался скитала, наматывали спиралью (виток к витку) полоску пергамента и писали на ней вдоль стержня несколько строк текста сообщения (рис.1). Затем снимали со стержня полоску пергамента с написанным текстом. Буквы на этой полоске оказывались расположенными хаотично. Такой же результат можно получить, если буквы сообщения писать по кольцу не подряд, а через определенное число позиций до тех пор, пока не будет исчерпан весь текст.

Рис. 1. Шифр "скитала"

Сообщение "НАСТУПАЙТЕ" при размещении его по окружности стержня по три буквы дает шифртекст:

НУТАПЕСА_ТЙ

Для расшифрования такого шифртекста нужно не только знать правило шифрования, но и обладать ключом в виде стержня определенного диаметра. Зная только вид шифра, но не имея ключа, расшифровать сообщение было непросто. Шифр "скитала" в последующие времена многократно совершенствовался.

Шифрующие таблицы

В эпоху Возрождения (с конца XIV в.) начала возрождаться и криптография. Наряду с традиционными вариантами применения криптографии в политике, дипломатии и военном деле появляются и другие - защита интеллектуальной собственности от инквизиции или от злоумышленников. В разработанных шифрах того времени применяются шифрующие таблицы, которые, в сущности, задают правила перестановки букв в сообщении.

В качестве ключа в шифрующих таблицах используются:

размер таблицы;

слово или фраза, задающие перестановку;

особенности структуры таблицы.

Одним из самых примитивных табличных шифров перестановки является простая перестановка, для которой ключом служит размер таблицы. Этот метод шифрования сходен с шифром "скитала". Например, сообщение:

"ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ"

записывается в таблицу поочередно по столбцам. Результат заполнения таблицы из 5 строк и 7 столбцов показан на рис. 2.

Т	**Н**	**П**	**В**	**Е**	**Г**	**Л**
Е	**А**	**Р**	**А**	**Д**	**О**	**Н**
Р	**Т**	**И**	**Е**	**Ь**	**В**	**О**
М	**О**	**Б**	**Т**	**М**	**П**	**Ч**
И	**Р**	**Ы**	**С**	**О**	**О**	**Ь**

Рис. 2. Заполнение таблицы из 5 строк и 7 столбцов

После заполнения таблицы текстом сообщения по столбцам для формирования шифртекста считывают содержимое таблицы по строкам. Если шифртекст записывать группами по пять букв, получается такое шифрованное сообщение:

ТНПВЕ ГЛЕАР АДОНР ТИЕЬВ ОМОБТ МПЧИР ЫСООЬ

Естественно, отправитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы. Следует заметить, что объединение букв шифртекста в 5-буквенные группы не входит в ключ шифра и осуществляется для удобства записи несмыслового текста. При расшифровке действия выполняют в обратном порядке.

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый "одиночная перестановка по ключу". Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Применим в качестве ключа, например, слово:

"ПЕЛИКАН",

а текст сообщения возьмем из предыдущего примера. На рис. 3 показаны две таблицы, заполненные текстом сообщения и ключевым словом, при этом левая таблица соответствует заполнению до перестановки, а правая - после перестановки.

КЛЮЧ

→

П	Е	Л	И	К	А	Н
7	2	5	3	4	1	6
Т	Н	П	В	Е	Г	Л
Е	А	Р	А	Д	О	Н
Р	Т	И	Е	Ь	В	О
М	О	Б	Т	М	П	Ч
И	Р	Ы	С	О	О	Ь

А	Е	И	К	Л	Н	П
1	2	3	4	5	6	7
Г	Н	В	Е	П	Л	Т
О	А	А	Д	Р	Н	Е
В	Т	Е	Ь	И	О	Р
П	О	Т	М	Б	Ч	М
О	Р	С	О	Ы	Ь	И

После перестановки

До перестановки

Рис 3. Таблицы, заполненные ключевым словом и текстом сообщения

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если бы в ключе встретились одинаковые буквы, они бы были понумерованы слева направо. В правой таблице столбцы переставлены в соответствии с упорядоченными номерами букв ключа.

При считывании содержимого правой таблицы по строкам и записи шифртекста группами по пять букв получим шифрованное сообщение:

ГНВЕП ЛТОАА ДРНЕВ ТЕЬИО РПОТМ БЧМОР СОЫЬИ

Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется **двойной перестановкой**. В этом случае перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок должен быть обратным.

Пример выполнения шифрования методом двойной перестановки показан на рис. 4. Если считывать шифртекст из правой таблицы построчно блоками по четыре буквы, то получится следующее:

ТЮАЕ ООГМ РЛИП ОЬСВ

Ключом к шифру двойной перестановки служит последовательность номеров столбцов и номеров строк исходной таблицы (в нашем примере последовательности 4132 и 3142 соответственно).

	4	1	3	2
3	*П*	**Р**	**И**	**Л**
1	**Е**	**Т**	**А**	**Ю**
4	**В**	**О**	**С**	**Ь**
2	**М**	**О**	**Г**	**О**

Исходная таблица

	1	2	3	4
3	**Р**	**Л**	**И**	*П*
1	**Т**	**Ю**	**А**	**Е**
4	**О**	**Ь**	**С**	**В**
2	**О**	**О**	**Г**	**М**

Перестановка столбцов

	1	2	3	4
1	**Т**	**Ю**	**А**	**Е**
2	**О**	**О**	**Г**	**М**
3	**Р**	**Л**	**И**	*П*
4	**О**	**Ь**	**С**	**В**

Перестановка строк

Рис. 4. Пример выполнения шифрования методом двойной перестановки

Число вариантов двойной перестановки быстро возрастает при увеличении размера таблицы:

для таблицы 3x3 - 36 вариантов;

для таблицы 4x4 - 576 вариантов;

для таблицы 5x5 - 14400 вариантов.

Однако двойная перестановка не отличается высокой стойкостью и сравнительно просто "взламывается" при любом размере таблицы шифрования.

Магические квадраты

В средние века для шифрования перестановкой применялись "магические квадраты". Так называют квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Шифруемый текст вписывали в "магические квадраты" в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный благодаря перестановке букв исходного сообщения. В те времена считалось, что созданные с помощью "магических квадратов" шифртексты охраняет не только ключ, но и магическая сила.

Пример "магического квадрата" и его заполнения сообщением **"ПРИЛЕТАЮ ВОСЬМОГО"** показан на рис. 5.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

О	И	Р	М
Е	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

Рис 5. Пример "магического квадрата" 4х4 и его заполнения

Шифртекст, получаемый при считывании содержимого правой таблицы по строкам, имеет вполне загадочный вид:

ОИРМ ЕОСЮ ВТАЬ ЛГОП

Число "магических квадратов" быстро возрастает с увеличением размера квадрата. Существует только один "магический квадрат" размером 3х3 (если не учитывать его повороты). Количество "магических квадратов" 4х4 составляет уже 880, а количество магических квадратов 5х5 - около 250000.

Магические квадраты средних и больших размеров могли служить хорошей базой для обеспечения нужд шифрования того времени, поскольку практически нереально выполнить вручную перебор всех вариантов для такого шифра.

Задание.

1. Зашифровать 81 символ текста методом одиночной перестановки по ключу (см. рис. 3). Нумерацию символов ключевого слова проводить по табл. 1. Знаки препинания и пробелы не учитывать.

2. Поменяться с соседом зашифрованными текстами и ключами. Расшифровать текст.

Таблица 1

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
А	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**Й**	**К**	**Л**	**М**	**Н**	**О**	**П**

17	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**
Р	**С**	**Т**	**У**	**Ф**	**К**	**Ц**	**Ч**	**Ш**	**Щ**	**Ь**	**Ы**	**Ъ**	**Э**	**Ю**	**Я**

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Номер варианта	Текст	Ключевое слов
1.	ДУМАЕТСЯ, ЧТО КАЖДОМУ ЧИТАТЕЛЮ ДАННОГО ПОСОБИЯ ДОВОДИЛОСЬ СДАВАТЬ КАКИЕ-ЛИБО ЭКЗАМЕНЫ И ВЫ ВСЕ БОЛЕЕ ИЛИ МЕНЕЕ ПРЕДСТАВЛЯЕТЕ СЕБЕ, ЧТО ЭТО ТАКОЕ.	ДИПЛОМАНТ
2.	ТЕМ НЕ МЕНЕЕ, ДЛЯ РАЗРАБОТКИ ПОДЛИННО НАУЧНОГО ПОДХОДА НЕОБХОДИМО ТОЧНОЕ ОПРЕДЕЛЕНИЕ ИЗУЧАЕМОГО ЯВЛЕНИЯ.	КИМБЕРЛИТ
3.	БУДЬ Я МИНИСТРОМ ОБРАЗОВАНИЯ, ВО ВСЕХ ВУЗАХ ВВЕЛ БЫ В ОБЯЗАТЕЛЬНОМ ПОРЯДКЕ ИЗУЧЕНИЕ МЕТОДОВ ОТЛЫНИВАНИЯ, ТЕХНОЛОГИИ ИЗГОТОВЛЕНИЯ ШПАРГАЛОК И ИСКУССТВА ЛИТЬ ВОДУ, ПРИЧЕМ С ОБЯЗАТЕЛЬНЫМ ЭКЗАМЕНОМ	КРОНШТЕЙН
4.	ВООБРАЗИТЕ ОТРАДНУЮ КАРТИНУ: СТУДЕНТ, ИЗГОТОВЛЯЮЩИЙ "ШПОРЫ" НА ЭКЗАМЕН ПО ШПАРГАЛКОВЕДЕНИЮ	КРУПОЗНЫЙ
5.	И ДЕЙСТВИТЕЛЬНО, В ПРОЦЕССЕ ЭКЗАМЕНА ИСПЫТЫВАЮТСЯ САМЫЕ РАЗНООБРАЗНЫЕ КАЧЕСТВА СТУДЕНТА - ОТ ОРАТОРСКОГО МАСТЕРСТВА ДО ИСКУССТВА ПАНТОМИМЫ	МАССАЖИСТ
6.	СРАЗУ ХОЧУ ОТМЕТИТЬ МОЕ ПРИНЦИПИАЛЬНОЕ НЕСОГЛАСИЕ С ОБЩЕПРИНЯТЫМИ ТРАКТОВКАМИ, В КОТОРЫХ СТУДЕНТ ВЫСТУПАЕТ ПАССИВНЫМ ОБЪЕКТОМ, НАД КОТОРЫМ ЭКЗАМЕНАТОРЫ ПРОДЕЛЫВАЮТ КАКИЕ-ЛИБО ТОЛЬКО ИМ ПОДКОНТРОЛЬНЫЕ ДЕЙСТВИЯ	КРУПЧАТКА
7.	НАПРОТИВ, ИДЕАЛЬНЫЙ ЭКЗАМЕНАТОР ВЫПОЛНЯЕТ РОЛЬ БЕСПРИСТРАСТНОГО ИЗМЕРИТЕЛЯ УРОВНЯ ЗНАНИЙ СТУДЕНТА	ЛАНДКАРТА
8.	СЛЕДУЕТ ПРИЗНАТЬ, ЧТО ТАКОЙ ТИП В ПРИРОДЕ НЕ ВСТРЕЧАЕТСЯ. ЭКЗАМЕНАТОР МОЖЕТ БЫТЬ НАСТРОЕН ПО ОТНОШЕНИЮ К СТУДЕНТУ ПОЛОЖИТЕЛЬНО ИЛИ ОТРИЦАТЕЛЬНО, НО ВЕДЬ ТАКИМ ЕГО ДЕЛАЕТ САМ СТУДЕНТ	ЛАМАРКИЗМ
9.	СЛЕДОВАТЕЛЬНО, ЭКЗАМЕН НАЧИНАЕТСЯ НЕ ТОГДА, КОГДА ВАША ДРОЖАЩАЯ РУКА ТЯНЕТСЯ ЗА БИЛЕТОМ, А ЕЩЕ ПРИ ПЕРВОЙ ВСТРЕЧЕ СТУДЕНТА С БУДУЩИМ ЭКЗАМЕНАТОРОМ	ЛАКРИНЧИК
10.	ЭКЗАМЕН МОЖНО ОПРЕДЕЛИТЬ КАК СОВОКУПНОСТЬ ДЕЙСТВИЙ СТУДЕНТА, НАПРАВЛЕННЫХ НА ТО, ЧТОБЫ ЭКЗАМЕНАТОР ПОСЧИТАЛ ЕГО ДОСТОЙНЫМ КАК МОЖНО БОЛЕЕ ВЫСОКОЙ ОЦЕНКИ	ОРТОПЕДИЯ
11.	ДО СИХ ПОР Я ЧАСТО ВСПОМИНАЮ СВОЙ ПОСЛЕДНИЙ ШКОЛЬНЫЙ ЭКЗАМЕН ПО ФИЗИКЕ.	СЕРПОВИЩЕ

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
		ПРИНИМАЛА ЕГО УЧИТЕЛЬНИЦА, ТВЕРДО УВЕРЕННАЯ В МОИХ ГЛУБОКИХ ПОЗНАНИЯХ В ЭТОЙ ОБЛАСТИ													
12.		ВОЛЕЙ СУДЕБ МНЕ ПРИШЛОСЬ ОТВЕЧАТЬ НА ВОПРОС О ФИЛОСОФСКИХ КОНЦЕПЦИЯХ, ПРИМЕНИМЫХ В ФИЗИКЕ. ОБ ЭТОМ Я НЕ ЗНАЛ АБСОЛЮТНО НИЧЕГО											СУСПЕНЗИЯ		
13.		ДЛЯ ТОГО, ЧТОБЫ РАССМАТРИВАТЬ В ДАЛЬНЕЙШЕМ ВОПРОСЫ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ, НЕОБХОДИМО НАПОМНИТЬ ОСНОВНЫЕ ПОНЯТИЯ, КОТОРЫМИ ОПЕРИРУЕТ ТЕОРИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ											ОБРАБОТКА		
14.		ОСНОВНОЙ ОСОБЕННОСТЬЮ ЛЮБОЙ СЕТЕВОЙ СИСТЕМЫ ЯВЛЯЕТСЯ ТО, ЧТО ЕЕ КОМПОНЕНТЫ РАСПРЕДЕЛЕНЫ В ПРОСТРАНСТВЕ И СВЯЗЬ МЕЖДУ НИМИ ФИЗИЧЕСКИ ОСУЩЕСТВЛЯЕТСЯ ПРИ ПОМОЩИ СЕТЕВЫХ СОЕДИНЕНИЙ											ОПАСНОСТЬ		
15.		УГРОЗА БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СИСТЕМЫ - ЭТО ПОТЕНЦИАЛЬНО ВОЗМОЖНОЕ ПРОИСШЕСТВИЕ, НЕВАЖНО, ПРЕДНАМЕРЕННОЕ ИЛИ НЕТ, КОТОРОЕ МОЖЕТ ОКАЗАТЬ НЕЖЕЛАТЕЛЬНОЕ ВОЗДЕЙСТВИЕ НА САМУ СИСТЕМУ, А ТАКЖЕ НА ИНФОРМАЦИЮ, ХРАНЯЩУЮСЯ В НЕЙ											СОВЕТСКИЙ		
16.		УЯЗВИМОСТЬ КОМПЬЮТЕРНОЙ СИСТЕМЫ - ЭТО НЕКАЯ ЕЕ НЕУДАЧНАЯ ХАРАКТЕРИСТИКА, КОТОРАЯ ДЕЛАЕТ ВОЗМОЖНЫМ ВОЗНИКНОВЕНИЕ УГРОЗЫ											ОТНОШЕНИЕ		
17.		УГРОЗА ОТКАЗА В ОБСЛУЖИВАНИИ ВОЗНИКАЕТ ВСЯКИЙ РАЗ, КОГДА В РЕЗУЛЬТАТЕ НЕКОТОРЫХ ДЕЙСТВИЙ БЛОКИРУЕТСЯ ДОСТУП К НЕКОТОРОМУ РЕСУРСУ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ											ИЕРУСАЛИМ		
18.		АТАКА НА КОМПЬЮТЕРНУЮ СИСТЕМУ - ЭТО ДЕЙСТВИЕ, ПРЕДПРИНИМАЕМОЕ ЗЛОУМЫШЛЕННИКОМ, КОТОРОЕ ЗАКЛЮЧАЕТСЯ В ПОИСКЕ И ИСПОЛЬЗОВАНИИ ТОЙ ИЛИ ИНОЙ УЯЗВИМОСТИ											НАЧАЛЬНИК		
19.		ИССЛЕДОВАТЕЛИ ОБЫЧНО ВЫДЕЛЯЮТ ТРИ ОСНОВНЫХ ВИДА УГРОЗ БЕЗОПАСНОСТИ - ЭТО УГРОЗЫ РАСКРЫТИЯ, ЦЕЛОСТНОСТИ И ОТКАЗА В ОБСЛУЖИВАНИИ											ПОКОЛЕНИЕ		
20.		В ТЕРМИНАХ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ УГРОЗА РАСКРЫТИЯ ИМЕЕТ МЕСТО ВСЯКИЙ РАЗ, КОГДА ПОЛУЧЕН ДОСТУП К НЕКОТОРОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ХРАНЯЩЕЙСЯ В ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ ИЛИ ПЕРЕДАВАЕМОЙ ОТ ОДНОЙ СИСТЕМЫ К											КОНЦЕПЦИЯ		

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
		ДРУГОЙ													
	21.	УГРОЗА ЦЕЛОСТНОСТИ ВКЛЮЧАЕТ В СЕБЯ ЛЮБОЕ УМЫШЛЕННОЕ ИЗМЕНЕНИЕ ДАННЫХ, ХРАНЯЩИХСЯ В ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ ИЛИ ПЕРЕДАВАЕМЫХ ИЗ ОДНОЙ СИСТЕМЫ В ДРУГУЮ											ОТНОШЕНИЕ		

Лабораторная работа 4. ИЗУЧЕНИЕ ТРАДИЦИОННЫХ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ. ШИФРЫ ЗАМЕНЫ

ШИФРЫ ПРОСТОЙ ЗАМЕНЫ

При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены. В шифре простой замены каждый символ исходного текста заменяется символами того же алфавита одинаково на всем протяжении текста. Часто шифры простой замены называют шифрами одноалфавитной подстановки.

Полибианский квадрат.

Одним из первых шифров простой замены считается так называемый *полибианский квадрат.* За два века до нашей эры греческий писатель и историк Полибий изобрел для целей шифрования квадратную таблицу размером 5x5, заполненную буквами греческого алфавита в случайном порядке (рис. 1).

λ	ε	υ	ω	γ
ρ	ζ	δ	σ	ο
μ	η	β	ξ	τ
ψ	π	θ	α	x
χ	ν		φ	ι

Рис. 1. Полибианский квадрат, заполненный случайным образом 24 буквами греческого алфавита и пробелом

При шифровании в этом полибианском квадрате находили очередную букву открытого текста и записывали в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывалась в нижней строке таблицы, то для шифртекста брали самую верхнюю букву из того же столбца. Например, для слова:

ταυροσ

получается шифртекст

χφδμτξ

Концепция полибианского квадрата оказалась плодотворной и нашла применение в криптосистемах последующего времени.

Система шифрования Цезаря.

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). Свое название он получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке с Цицероном (около 50 г. до н.э.).

При шифровании исходного текста каждая буква заменялась на другую букву того же алфавита по следующему правилу. Заменяющая буква определялась путем смещения по алфавиту от исходной буквы на **К** букв. При достижении конца алфавита выполнялся циклический переход к его началу. Цезарь использовал шифр замены при смещении **К = 3**. Такой шифр замены

можно задать таблицей подстановок, содержащей соответствующие пары букв открытого текста и шифртекста. Совокупность возможных подстановок для **К = 3** показана в табл. 1.

Таблица 1

Одноалфавитные подстановки (К = 3, m = 26).

A	→	**D**	**J**	→	**M**	**S**	→	**V**
B	→	**E**	**K**	→	**N**	**T**	→	**W**
C	→	**F**	**L**	→	**O**	**U**	→	**X**
D	→	**G**	**M**	→	**P**	**V**	→	**Y**
E	→	**H**	**N**	→	**Q**	**W**	→	**Z**
F	→	**I**	**O**	→	**R**	**X**	→	**A**
G	→	**J**	**P**	→	**S**	**Y**	→	**B**
H	→	**K**	**Q**	→	**T**	**Z**	→	**C**
I	→	**L**	**R**	→	**U**			

Например, послание Цезаря

"VENI VIDI VICI"

(в переводе на русский означает "Пришел, Увидел, Победил"), направленное его другу Аминтию после победы над понтийским царем Фарнаком, сыном Митридата, выглядело бы в зашифрован ном виде так:

YHQL YLGL YLFL

Достоинством системы шифрования Цезаря является простота шифрования и расшифровки. К недостаткам системы Цезаря следует отнести следующие:

подстановки, выполняемые в соответствии с системой Цезаря, не маскируют частот появления различных букв исходного открытого текста;

сохраняется алфавитный порядок в последовательности заменяющих букв; при изменении значения **К** изменяются только начальные позиции такой последовательности;

число возможных ключей **К** мало;

шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифртексте.

Криптоаналитическая атака против системы одноалфавитной замены начинается с подсчета частот появления символов: определяется число появлений каждой буквы в шифртексте. Затем полученное распределение частот букв в шифртексте сравнивается с распределением частот букв в алфавите исходных сообщений, например, в английском. Буква с наивысшей частотой по явления в шифртексте заменяется на букву с наивысшей частотой появления в английском языке и т.д. Вероятность успешного вскрытия системы шифрования повышается с увеличением длины шифртекста.

Концепция, заложенная в систему шифрования Цезаря, оказалась весьма плодотворной, о чем свидетельствуют ее многочисленные модификации.

Система Цезаря с ключевым словом

Система шифрования Цезаря с ключевым словом является одноалфавитной системой подстановки. Особенность этой системы - использование ключевого слова для смещения и изменения порядка символов в алфавите подстановки.

Выберем некоторое число **k, 0 ≤ k ≤ 25** и слово или короткую фразу в качестве ***ключевого слова***. Желательно, чтобы все буквы ключевого слова были различными. Пусть выбраны слово **DIPLOMAT** в качестве ключевого слова и число **k = 5**.

Ключевое слово записывается под буквами алфавита, начиная с буквы, числовой код которой совпадает с выбранным числом **k**:

0	1	2	3	4	5					10					15					20					25
A	B	C	D	E	F	H	G	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
					D	I	P	L	O	M	A	T													

Оставшиеся буквы алфавита подстановки записываются после ключевого слова в алфавитном порядке:

0	1	2	3	4	5					10					15					20					25
A	B	C	D	E	F	H	G	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	D	I	P	L	O	M	A	T	B	C	E	F	G	H	J	K	N	Q	R	S	U

Теперь мы имеем подстановку для каждой буквы произвольного сообщения.

Исходное сообщение **SEND MORE MONEY** шифруется как **HZBY TCGZ TCBZS.**

Следует отметить, что требование о различии всех букв ключевого слова не обязательно. Можно просто записать ключевое слово (или фразу) без повторения одинаковых букв. Например, ключевая фраза: "**КАК ДЫМ ОТЕЧЕСТВА НАМ СЛАДОК И ПРИЯТЕН"** и число **k = 3** порождают следующую таблицу подстановок:

0	1	2	3		5					10										20					25					30	
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
Ъ	Э	Ю	К	А	Д	Ы	М	О	Т	Е	Ч	С	В	Н	Л	И	П	Р	Я	Б	Г	Ж	З	Й	У	Ф	Х	Ц	Ш	Щ	Ь

Несомненное достоинство системы Цезаря с ключевым словом - то, что количество возможных ключевых слов практически неисчерпаемо. Недостат-

ком этой системы является возможность взлома шифртекста на основе анализа частот появления букв.

Шифрующие таблицы Трисемуса

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием "Полиграфия". В ней он впервые систематизировал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем таблица дополнялась не вошедшими в нее буквами алфавита по порядку.

Поскольку ключевое слово или фразу легко хранить в памяти, то такой подход упрощал процессы шифрования и расшифровки.

Поясним этот метод шифрования на примере. Для русско го алфавита шифрующая таблица может иметь размер 4x8. Берем в качестве ключа слово "БАНДЕРОЛЬ". Шифрующая таблица с таким ключом показана на рис. 2.

Б	*А*	Н	*Д*	*Е*	Р	О	Л
Ь	В	Г	Ж	З	И	И	К
М	П	С	Т	У	Ф	Х	Ц
Ч	Ш	Щ	Ы	Ъ	Э	Ю	Я

Рис. 2. Шифрующая таблица с ключевым словом "БАНДЕРОЛЬ"

Как и в случае полибианского квадрата, при шифровании находят в этой таблице очередную букву открытого текста и записывают в шифртекст букву, расположенную ниже ее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца. Например, при шифровании с помощью этой таблицы сообщения:

"ВЫЛЕТАЕМПЯТОГО"

получаем шифртекст:

"ПДКЗЫВЗЧШЛЫЙСЙ".

Такие табличные шифры называются монограммными, так как шифрование выполняется по одной букве. Трисемус первым заметил, что шифрующие таблицы позволяют шифровать сразу по две буквы. Такие шифры называются ***биграммными.***

Биграммный шифр Плейфейра.

Шифр Плейфейра, изобретенный в 1854 г. - наиболее известный биграммный шифр замены. Он применялся Великобританией во время первой мировой войны. Основой шифра является шифрующая таблица со случайно расположенными буквами алфавита исходных сообщений.

Для удобства запоминания шифрующей таблицы отправителем и получателем сообщений можно использовать ключевое слово (или фразу) при заполнении начальных строк таблицы. В целом структура шифрующей таблицы системы Плейфейра полностью аналогична структуре шифрующей таблицы Трисемуса. Поэтому для пояснения процедур шифрования и расшифрования в системе Плейфейра воспользуемся шифрующей таблицей Трисемуса из предыдущего раздела (см. рис 2.)

Процедура шифрования включает следующие этапы.

1. Открытый текст исходного сообщения разбивается на пары букв (биграммы). Текст должен иметь четное количество букв, и в нем не должно быть биграмм, содержащих две одинаковые буквы. Если эти требования не выполнены, то текст модифицируется даже из-за незначительных орфографических ошибок.

2. Последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы в последовательность биграмм шифртекста по следующим правилам:

а) если обе буквы биграммы открытого текста не попадают на одну строку или столбец (как, например, буквы А и И в табл. на рис.2), тогда находят буквы в углах прямоугольника, определяемого данной парой букв (в нашем примере это буквы АЙОВ. Пара букв АЙ отображается в пару 0В. Последовательность букв в биграмме шифртекста должна быть зеркально расположенной по отношению к последовательности букв в биграмме открытого текста);

б) если обе буквы биграммы открытого текста принадлежат одному столбцу таблицы, то буквами шифртекста считаются буквы, которые лежат под ними (например, биграмма НС дает биграмму шифртекста ГЩ); если при этом буква открытого текста находится в нижней строке, то для шифртекста берется соответствующая буква из верхней строки того же столбца (например, биграмма ВШ дает биграмму шифртекста ПА);

в) если обе буквы биграммы открытого текста принадлежат одной строке таблицы, то буквами шифртекста считаются буквы, которые лежат справа от них (например, биграмма НО дает биграмму шифртекста ДЛ); если при этом буква от крытого текста находится в крайнем правом столбце, то для шифра берут соответствующую букву из левого столбца в той же строке (например, биграмма ФЦ дает биграмму шифртекста ХМ.).

Зашифруем текст:

"ВСЕ ТАЙНОЕ СТАНЕТ ЯВНЫМ"

Разбиение этого текста на биграммы дает:

"ВС ЕТ АЙ НО ЕС ТА НЕ ТЯ ВН ЫМ"

Данная последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы (см. рис. 2.8) в следующую последовательность биграмм шифртекста:

"ГП ДУ 0В ДЛ НУ ПД ДР ЦЫ ГА ЧТ".

При расшифровке применяется обратный порядок действий.

Следует отметить, что шифрование биграммами резко повышает стойкость шифров к вскрытию. Хотя книга И. Трисемуса "Полиграфия" была от-

носительно доступной, описанные в ней идеи получили признание лишь спустя три столетия. По всей вероятности, это было обусловлено плохой осведомленностью криптографов о работах богослова и библиофила Трисемуса в области криптографии.

Шифры сложной замены

Шифры сложной замены называют многоалфавитными, так как для шифрования каждого символа исходного сообщения применяют свои шифр простой замены. Многоалфавитная подстановка последовательно и циклически меняет используемые алфавиты.

При **r** - алфавитной подстановке символ $\mathbf{x_0}$ исходного сообщения заменяется символом $\mathbf{y_0}$ из алфавита $\mathbf{B_0}$, символ $\mathbf{x_i}$ -символом **yi**, из алфавита $\mathbf{B_1}$, и так далее, символ $\mathbf{x}_{r-1}$ заменяется символом $\mathbf{y}_{r-1}$ из алфавита $\mathbf{B}_{r-1}$, символ $\mathbf{x}_r$ заменяется символом $\mathbf{y}_r$ снова из алфавита $\mathbf{B_0}$, и т.д.

Общая схема многоалфавитной подстановки для случая r = 4 показана на рис.3.

Входной символ	$\mathbf{X_0}$	$\mathbf{X_1}$	$\mathbf{X_2}$	$\mathbf{X_3}$	$\mathbf{X_4}$	$\mathbf{X_5}$	$\mathbf{X_6}$	$\mathbf{X_7}$	$\mathbf{X_8}$	$\mathbf{X_9}$
Алфавит Подстановки	$\mathbf{B_0}$	$\mathbf{B_1}$	$\mathbf{B_2}$	$\mathbf{B_3}$	$\mathbf{B_0}$	$\mathbf{B_1}$	$\mathbf{B_2}$	$\mathbf{B_3}$	$\mathbf{B_0}$	$\mathbf{B_1}$

Рид. 3. Схема r-алфавитной подстановки для случая **r = 4**

Эффект использования многоалфавитной подстановки заключается в том, что обеспечивается маскировка естественной статистики исходного языка, так как конкретный символ из исходного алфавита **A** может быть преобразован в несколько различных символов шифровальных алфавитов $\mathbf{B_j}$. Степень обеспечиваемой защиты теоретически пропорциональна длине периода **r** в последовательности используемых алфавитов $\mathbf{B_j}$.

Многоалфавитные шифры замены предложил и ввел в практику криптографии Леон Батист Альберти, который также был известным архитектором и теоретиком искусства. Его книга "Трактат о шифре", написанная в 1566 г., представляла собой первый в Европе научный труд по криптологии. Кроме шифра многоалфавитной замены, Альберти подробно описал устройства из вращающихся колес для его реализации. Во всем мире Л.Альберти почитается основоположником криптологии.

Шифр Гронсфельда

Этот шифр сложной замены представляет собой модификацию шифра Цезаря числовым ключом. Под буквами исходного сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифртекст получают примерно как в шифре Цезаря, но отсчитывают по алфавиту не третью букву (как в шифре Цезаря), а выбирают ту букву, которая смещена по алфавиту на соответствующую цифру ключа. Например, применяя в качестве ключа группу из четырех начальных цифр

числа **е** (основания натуральных логарифмов – 2718), получаем для исходного сообщения "**ВОСТОЧНЫЙ ЭКСПРЕСС"** следующий шифртекст:

Сообщение	**В**	**О**	**С**	**Т**	**О**	**Ч**	**Н**	**Ы**	**Й**	**Э**	**К**	**С**	**П**	**Р**	**Е**	**С**	**С**
Ключ	**2**	**7**	**1**	**8**	**2**	**7**	**1**	**8**	**2**	**7**	**1**	**8**	**2**	**7**	**1**	**8**	**2**
Шифртекст	**Д**	**Х**	**Т**	**Ь**	**Р**	**Ю**	**О**	**Г**	**Л**	**Д**	**Л**	**Щ**	**С**	**Ч**	**Ж**	**Щ**	**У**

Чтобы зашифровать первую букву сообщения (В), используя первую цифру ключа 2, нужно отсчитать вторую по порядку букву от В в алфавите В-Г-Д; получается первая буква шифртекста - Д.

Следует отметить, что шифр Гронсфельда вскрывается относительно легко, если учесть, что в числовом ключе каждая цифра имеет только десять значений, а значит есть лишь десять вариантов прочтения каждой буквы шифртекста. С другой стороны, шифр Гронсфельда допускает дальнейшие модификации, улучшающие его стойкость, в частности двойное шифрование разными числовыми ключами.

По существу шифр Гронсфельда представляет собой частный случай системы шифрования Вижинера.

Система шифрования Вижинера

Система Вижинера, впервые опубликованная в 1586 г., является одной из старейших и наиболее известных многоалфавитных систем. Свое название она получила по имени французского дипломата XVI в. Блеза Вижинера, который развивал и совершенствовал криптографические системы.

Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены можно описать таблицей шифрования, называемой таблицей (квадратом) Вижинера. На рис. 4 показана таблица Вижинера для русского алфавита.

Таблица Вижинера используется для зашифрования и расшифровки. Таблица имеет два входа:

верхнюю строку подчеркнутых символов, используемую для считывания очередной буквы исходного открытого текста;

крайний левый столбец ключа.

Ключ	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
0	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я
1	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А
2	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б
3	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В
4	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г
5	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д
6	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е
7	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
8	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З

9	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
10	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
11	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
12	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
13	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
14	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
15	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
16	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
17	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
18	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
19	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
20	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
21	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
22	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
23	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
24	Ш	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
25	Щ	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
26	Ь	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
27	Ы	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь
28	Ъ	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы
29	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ
30	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э
31	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Ъ	Э	Ю

Рис. 4. Таблица Вижинера

Последовательность ключей обычно получают из числовых значений букв ключевого слова.

При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово (или фразу). Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

Таблица Вижинера для английского алфавита составляется аналогичным образом.

Рассмотрим пример получения шифртекста с помощью таблицы Вижинера. Пусть выбрано ключевое слово "АМБРОЗИЯ". Необходимо зашифровать сообщение "ПРИЛЕТАЮ СЕДЬМОГО".

Выпишем исходное сообщение в строку и запишем под ним ключевое слово с повторением. В третью строку будем выписывать буквы шифртекста, определяемые из таблицы Вижинера.

Сообщение	П	Р	И	Л	Е	Т	А	Ю	С	Е	Д	Ь	М	О	Г	О
Ключ	А	М	Б	Р	О	З	И	Я	А	М	Б	Р	О	З	И	Я
Шифртекст	П	Ъ	Й	Ы	У	Щ	И	Э	С	С	Е	К	Ь	Х	Л	Н

Шифр "двойной квадрат" Уитстона

В 1854 г. англичанин Чарльз Уитстон разработал новый метод шифрования биграммами, который называют "двойным квадратом". Свое название этот шифр получил по аналогии с полибианским квадратом. Шифр Уитстона открыл новый этап в истории развития криптографии. В отличие от полибианского шифр "двойной квадрат" использует сразу две таблицы, размещенные по одной горизонтали, а шифрование идет биграммами, как в шифре Плейфейра. Эти не столь сложные модификации привели к появлению на свет качественно новой криптографической системы ручного шифрования. Шифр "двойной квадрат" оказался очень надежным и удобным и применялся Германией даже в годы второй мировой войны.

Поясним на примере процедуру шифрования этим шифром. Пусть имеются две таблицы со случайно расположенными в них русскими алфавитами (рис. 5). Перед шифрованием исходное сообщение разбивают на биграммы. Каждая из них шифруется отдельно. Первую букву биграммы находят в левой таблице, а вторую - в правой. Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.

Ж	Щ	Н	Ю	Р
И	Т	Ь	Ц	Б
Я	М	Е	.	С
В	Ы	П	Ч	
:	Д	У	О	К
З	Э	Ф	Г	Ш
Х	А	,	Л	Ъ

И	Ч	Г	Я	Т
,	Ж	Ь	М	О
З	Ю	Р	В	Щ
Ц	:	П	Е	Л
Ъ	А	Н	.	Х
Э	К	С	Ш	Д
Б	Ф	У	Ы	

Рис. 5. Две таблицы со случайно расположенными символами русского алфавита для шифра "двойной квадрат"

Предположим, что шифруется биграмма исходного текста "ИЛ". Буква И находится в столбце 1 и строке 2 левой таблицы, буква Л находится в столбце 5 и строке 4 правой таблицы. Это означает, что прямоугольник образован строками 2 и 4, а также столбцами 1 левой таблицы и 5 правой таблицы. Следовательно, в биграмму шифртекста входят буква О, расположенная в столбце 5 и строке 2 правой таблицы, и буква В, расположенная в столбце 1 и строке 4 левой таблицы, т.е. получаем биграмму шифртекста 0В.

Если обе буквы биграммы сообщения лежат в одной строке, то и буквы шифртекста берут из той же строки. Первую букву биграммы шифртекста берут из левой таблицы в столбце, соответствующем второй букве биграммы сообщения; вторая буква берется из правой таблицы в столбце, со ответствующем первой букве биграммы сообщения. Поэтому биграмма сообщения ТО превращается в биграмму шифртекста ЖБ. Аналогичным образом шифруются все биграммы сообщения:

Шифрование методом "двойного квадрата" дает весьма устойчивый к вскрытию и простой в применении шифр. Взламывание шифртекста "двойного квадрата" требует больших усилий, при этом длина сообщения должна быть не менее 30 строк.

Задание

1. Зашифровать текст при помощи таблицы Вижинера (см. рис. 4), используя ключевое слово.

2. Обменяться с партнером зашифрованными тестами и ключевыми словами. Расшифровать текст.

Номер варианта	Текст	Ключевое слово
1.	СТЕГАНОГРАФИЯ СЛУЖИТ ДЛЯ ПЕРЕДАЧИ СЕКРЕТОВ В ДРУГИХ СООБЩЕНИЯХ	АБОНЕНТ
2.	КАК ПРАВИЛО ОТПРАВИТЕЛЬ ПИШЕТ КАКОЕ-НИБУДЬ НЕПРИМЕТНОЕ СООБЩЕНИЕ	СИСТЕМА
3.	ПРИЕМЫ ВКЛЮЧАЮТ НЕВИДИМЫЕ ЧЕРНИЛА, МАЛОПРИМЕТНЫЕ ПОМЕТКИ У БУКВ	РЕШЕНИЕ
4.	В НАСТОЯЩЕЕ ВРЕМЯ ЛЮДИ НАЧАЛИ ПРЯТАТЬ СЕКРЕТЫ В ГРАФИЧЕСКИХ ИЗОБРАЖЕНИЯХ	ТЕХНИКА
5.	В **ПЕРЕСТАНОВОЧНОМ ШИФРЕ** МЕНЯЕТСЯ НЕ ОТКРЫТЫЙ ТЕКСТ, А ПОРЯДОК СИМВОЛОВ	ПАРТНЕР
6.	КРИПТОГРАФИЯ РЕШАЕТ ПРОБЛЕМЫ СЕКРЕТНОСТИ, ПРОВЕРКИ ПОДЛИННОСТИ, ЦЕЛОСТНОСТИ	ФИНАНСЫ
7.	ПРОТОКОЛ - ЭТО ПОРЯДОК ДЕЙСТВИЙ, ПРЕДПРИНИМАЕМЫХ ДВУМЯ ИЛИ БОЛЕЕ СТОРОНАМИ	АУКЦИОН
8.	ДЕЙСТВИЕ ДОЛЖНО ВЫПОЛНЯТЬСЯ В СВОЮ ОЧЕРЕДЬ И ПОСЛЕ ОКОНЧАНИЯ ПРЕДЫДУЩЕГО	УСЛОВИЕ
9.	КАЖДЫЙ УЧАСТНИК ПРОТОКОЛА ДОЛЖЕН СОГЛАСИТЬСЯ СЛЕДОВАТЬ ПРОТОКОЛУ	ДЕВУШКА
10.	КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ - ЭТО ПРОТОКОЛ, ИСПОЛЬЗУЮЩИЙ КРИПТОГРАФИЮ	ПРИНЦИП
11.	ПОНЯТИЕ **ОДНОНАПРАВЛЕННОЙ ФУНКЦИИ** ЯВЛЯЕТСЯ ЦЕНТРАЛЬНЫМ В КРИПТОГРАФИИ	ЭКСПЕРТ
12.	ЗНАЮЩИЙ КОМБИНАЦИЮ ЧЕЛОВЕК МОЖЕТ ОТКРЫТЬ СЕЙФ, ПОЛОЖИТЬ В НЕГО ДОКУМЕНТ	ПОЛИЦИЯ
13.	ВСКРЫТИЕ С ВЫБРАННЫМ ОТКРЫТЫМ ТЕКСТОМ МОЖЕТ БЫТЬ ОСОБЕННО ЭФФЕКТИВНЫМ	БУДУЩЕЕ
14.	ИЗ-ЗА НЕДОСТАТКОВ СИСТЕМЫ СИНХРОНИЗАЦИЯ ЧАСОВ МОЖЕТ БЫТЬ НАРУШЕНА	УГЛЕКОП
15.	ОБЫЧНАЯ КРИПТОГРАФИЯ С ОТКРЫТЫМИ КЛЮЧАМИ ИСПОЛЬЗУЕТ ДВА КЛЮЧА	НАПИТОК
16.	ХАКЕР НЕ ПРЕНЕБРЕГАЕТ ОПЕРАТИВНО-ТЕХНИЧЕСКИМИ И АГЕНТУРНЫМИ МЕТОДАМИ	БОТИНОК
17.	ЕСЛИ ВНЕДРЕНИЕ ЗАКЛАДКИ ПРОХОДИТ УСПЕШНО, ВТОРАЯ АТАКА УЖЕ НЕ ТРЕБУЕТСЯ	ДЕРЗКИЙ

Номер варианта	Текст	Ключевое слово
18.	ХАКЕР ЗАРАНЕЕ ПРОДУМЫВАЕТ ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ НЕУДАЧИ	СИМПТОМ
19.	ПРОГРАММНАЯ ЗАКЛАДКА, ВНЕДРЕННАЯ В СИСТЕМУ, ЗАМЕТНА ТОЛЬКО ХАКЕРУ	ЧЕМОДАН
20.	С ТОЧКИ ЗРЕНИЯ ДРУГИХ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМА РАБОТАЕТ КАК ОБЫЧНО	ЭСКУЛАП
21.	ЕСЛИ АТАКА НЕ УДАЛАСЬ, ХАКЕР СТАРАЕТСЯ ОСТАВИТЬ ЛОЖНЫЙ СЛЕД	ВПАДИНА

Лабораторная работа 5. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации

Содержание задания

1. Программа должна обеспечивать работу в двух режимах: администратора (пользователя с фиксированным именем ADMIN) и обычного пользователя.
2. В режиме администратора программа должна поддерживать следующие функции (при правильном вводе пароля):

- смена пароля администратора (при правильном вводе старого пароля);
- просмотр списка имен зарегистрированных пользователей и установленных для них параметров (блокировка учетной записи, включение ограничений на выбираемые пароли) – всего списка целиком в одном окне или по одному элементу списка с возможностью перемещения к его началу или концу;
- добавление уникального имени нового пользователя к списку с пустым паролем (строкой нулевой длины);
- блокирование возможности работы пользователя с заданным именем;
- включение или отключение ограничений на выбираемые пользователем пароли (в соответствии с индивидуальным заданием, определяемым номером варианта);
- завершение работы с программой.

3. В режиме обычного пользователя программа должна поддерживать только функции смены пароля пользователя (при правильном вводе старого пароля) и завершения работы, а все остальные функции должны быть заблокированы.
4. После своего запуска программа должна запрашивать у пользователя в специальном окне входа ввод его имени и пароля. При вводе пароля его символы всегда должны на экране заменяться символом ‘*’.
5. При отсутствии введенного в окне входа имени пользователя в списке зарегистрированных администратором пользователей программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода имени или завершения работы с программой.

6. При неправильном вводе пароля программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода. При трехкратном вводе неверного пароля работа программы должна завершаться.
7. При первоначальном вводе пароля (обязательном при первом входе администратора или пользователя с зарегистрированным ранее администратором именем) и при дальнейшей замене пароля программа должна просить пользователя подтвердить введенный пароль путем его повторного ввода.
8. Если выбранный пользователем пароль не соответствует требуемым ограничениям (при установке соответствующего параметра учетной записи пользователя), то программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность ввода другого пароля, завершения работы с программой (при первом входе данного пользователя) или отказа от смены пароля.
9. Информация о зарегистрированных пользователях, их паролях, отсутствии блокировки их работы с программой, а также включении или отключении ограничений на выбираемые пароли должна сохраняться в специальном файле. При первом запуске программы этот файл должен создаваться автоматически и содержать информацию только об администраторе, имеющем пустой пароль.
10. Интерфейс с программой должен быть организован на основе меню, обязательной частью которого должно являться подменю «Справка» с командой «О программе». При выборе этой команды должна выдаваться информация об авторе программы и выданном индивидуальном задании. Интерфейс пользователя программы может также включать панель управления с дублирующими команды меню графическими кнопками и строку состояния.
11. Для реализации указанных в пунктах 2-3 функций в программе должны использоваться специальные диалоговые формы, позволяющие пользователю (администратору) вводить необходимую информацию.

Индивидуальные варианты заданий (ограничения на выбираемые пароли)

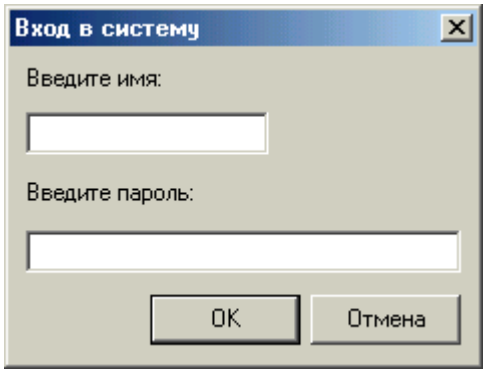
Длина не меньше минимальной длины, устанавливаемой администратором и сохраняемой в учетной записи пользователя.

1. Наличие строчных и прописных букв.
2. Наличие букв и цифр.
3. Наличие букв и знаков препинания.
4. Наличие цифр и знаков препинания.
5. Наличие букв и знаков арифметических операций.
6. Наличие цифр и знаков арифметических операций.
7. Наличие латинских букв и символов кириллицы.
8. Наличие букв, цифр и знаков препинания.
9. Наличие латинских букв, символов кириллицы и цифр.
10. Наличие латинских букв, символов кириллицы и знаков препинания.
11. Наличие строчных и прописных букв, а также цифр.

12. Наличие строчных и прописных букв, а также знаков препинания.
13. Наличие строчных и прописных букв, а также знаков арифметических операций.
14. Наличие латинских букв, символов кириллицы и знаков арифметических операций.
15. Наличие букв, цифр и знаков арифметических операций.
16. Наличие букв, знаков препинания и знаков арифметических операций.
17. Наличие цифр, знаков препинания и знаков арифметических операций.
18. Отсутствие повторяющихся символов.
19. Чередование букв, цифр и снова букв.
20. Чередование букв, знаков препинания и снова букв.
21. Чередование цифр, букв и снова цифр.
22. Отсутствие подряд расположенных одинаковых символов.
23. Чередование цифр, знаков препинания и снова цифр.
24. Чередование цифр, знаков арифметических операций и снова цифр.
25. Несовпадение с именем пользователя.

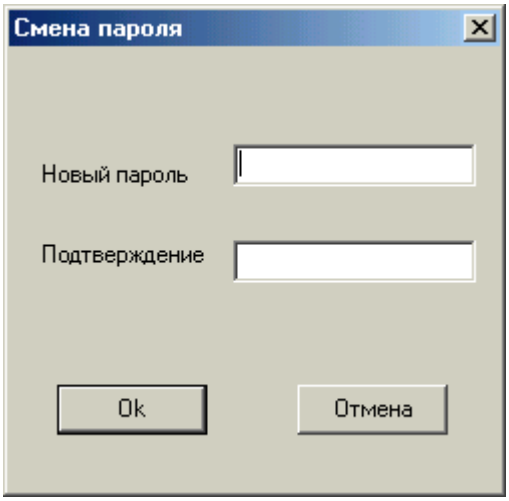
Возможный вид диалоговых форм программы

Окно входа в программу



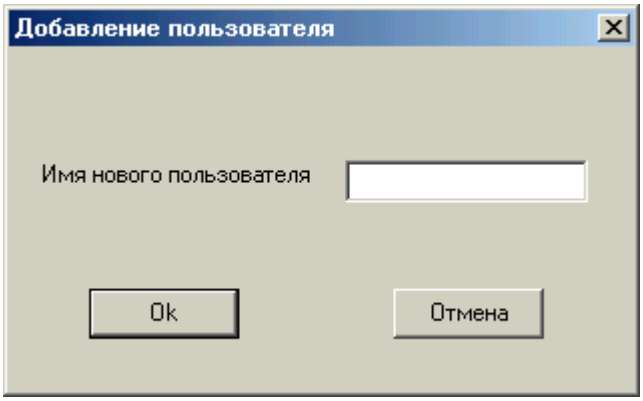
Может быть создано на основе шаблона Password Dialog, выбираемого с помощью команды File | New | Dialogs систем программирования Borland Delphi или Borland C++ Builder.

Окно смены пароля



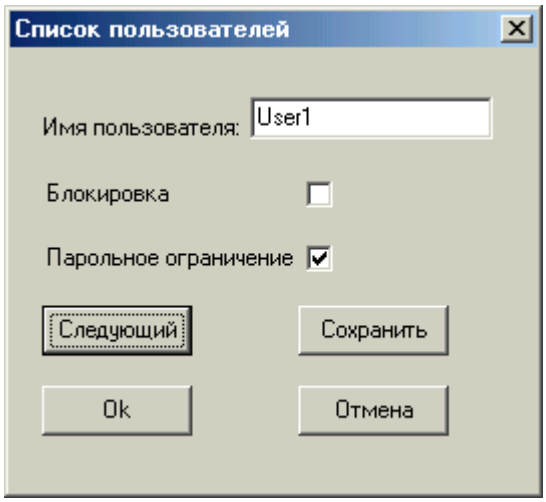
Возможно добавление на форму надписи «Старый пароль» и редактируемой строки для ввода действующего пароля.

Окно добавление нового пользователя



Возможно добавление на форму элементов управления для отображения и изменения значений параметров, устанавливаемых администратором для новой учетной записи (блокировка, ограничение на выбираемые пароли).

Окно просмотра (редактирования) учетных записей



Возможно добавление кнопки «Предыдущий» для перехода к предыдущей учетной записи или отображение списка учетных записей пользователей и их параметров в одном окне с помощью компонента StringGrid (группа Additional) систем программирования Borland Delphi или Borland C++ Builder.

Лабораторная работа 6. Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей

Содержание задания

1. Запустить программы просмотра и редактирования реестра Windows regedit.exe и regedt32.exe (с помощью команды «Выполнить» главного меню). Ознакомиться со структурой реестра, включить в отчет краткие сведения о содержании основных разделов реестра (HKEY_CURRENT_USER и HKEY_LOCAL_MACHINE). Включить в отчет сведения о различиях в функциональных возможностях изученных программ редактирования реестра. Включить в электронную версию отче-

та копии экранных форм, иллюстрирующих использование редакторов реестра.

Примечание: в операционную систему Windows XP Professional включен один редактор реестра, который можно запустить с помощью любого из указанных выше имен.

2. Скопировать в произвольную папку на диске рабочей станции файл rt.zip из указанного преподавателем сетевого диска.
3. Извлечь файлы из скопированного в пункте 2 архива.
4. Запустить программу restrick.exe, позволяющую ограничить возможности пользователей ОС Windows. Включить в отчет сведения о назначении и основных функциях программы. С помощью редактора реестра найти и отразить в отчете разделы реестра Windows, хранящие информацию о выбранной политике безопасности. Включить в отчет ответ на вопрос, какое ограничение на работу пользователя должно быть обязательно установлено, чтобы обеспечить минимальную эффективность рассмотренных и аналогичных средств. Включить в электронную версию отчета копии экранных форм, используемых при работе с программой restrick.exe. Завершить работу с программой restrick.exe.
5. Заблокировать работу с используемой рабочей станцией на период временного отсутствия пользователя. Разблокировать работу рабочей станции. Включить в отчет сведения о порядке защиты рабочей станции на период временного отсутствия пользователя и о других функциях операционной системы, доступных при этом наряду с блокировкой.
6. Открыть (или создать) произвольный документ в текстовом процессоре Word. Изучить порядок использования паролей для защиты документов в Microsoft Word и включить в отчет соответствующие сведения. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с Word.
7. Открыть (или создать) произвольную таблицу Excel. Изучить порядок использования паролей для защиты документов в табличном процессоре Microsoft Excel и включить в отчет соответствующие сведения. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с Excel.
8. Скопировать в произвольную папку на локальном жестком диске файл whisper.zip из указанного преподавателем сетевого диска.
9. Запустить программу Setup для установки программы Whisper 32 (непосредственно из архива, скопированного в пункте 8, без его распаковки).
10. Запустить программу whisper.exe, предназначенную для создания и ведения базы данных паролей пользователя. Изучить назначение и основные функции программы и включить в отчет соответствующие сведения. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с программой whisper.exe.

11. Ознакомиться (на примере папок, созданных в папке c:\ Documents and Settings \ *Имя пользователя* \ Документы и в папке c:\ Documents and Settings \ All Users \ Документы) с порядком разграничения доступа к ресурсам в защищенных версиях операционной системы Windows (с помощью контекстного меню объекта и элементов управления соответствующих диалоговых окон). Если команда «Общий доступ и безопасность» недоступна (при работе в ОС Windows XP Professional), то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки. Включить в отчет сведения об особенностях управления доступом к папкам и файлам в этих ОС. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта.
12. Ознакомиться (с помощью Панели управления Windows и редактора реестра) с порядком разграничения доступа к принтерам и разделам реестра. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта.
13. Ознакомиться (с помощью функции Панели управления Администрирование | Управление компьютером) с порядком создания и изменения учетных записей пользователей и групп в защищенных версиях операционной системы Windows. Включить в отчет соответствующие сведения. Включить в электронную версию отчета копии соответствующих экранных форм.
14. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Локальные политики | Назначение прав пользователя) с порядком назначения прав пользователям и группам. Включить в отчет соответствующие сведения. Включить в электронную версию отчета копии соответствующих экранных форм.
15. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика паролей) с порядком определения параметров безопасности для парольной аутентификации. Включить в отчет соответствующие сведения. Включить в электронную версию отчета копии соответствующих экранных форм.
16. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика блокировки учетных записей) с порядком определения параметров безопасности для политики блокировки учетных записей. Включить в отчет соответствующие сведения. Включить в электронную версию отчета копии соответствующих экранных форм.
17. Включить в отчет ответы на контрольные вопросы, номера которых выбираются в соответствии с номером варианта.
18. Включить в отчет титульный лист и сохранить файл с электронной версией отчета в произвольной папке на локальном жестком диске.
19. После проверки отчета преподавателем удалить файл с электронной версией отчета и файл программы Restrick, удалить программу Whisper 32 с

помощью Панели управления Windows, удалить файлы архивов rt.zip и whisper.zip.

20. Завершить работу с ОС Windows.

Контрольные вопросы

1. Какой из изученных в лабораторной работе редакторов реестра предоставляет функции по разграничению доступа к разделам реестра и как использовать эти функции?
2. Полномочия какого из пользователей ограничиваются с помощью программы restrick.exe?
3. В чем разница между функциями программы restrick.exe «Restrict “Run program” window» и «Restrict “Run” command»?
4. Как с помощью программы restrick.exe ограничить доступ пользователей к дисковым устройствам?
5. Как ограничить доступ пользователей к функциям Панели управления с помощью программы restrick.exe?
6. Доступ к каким функциям Панели управления может быть ограничен с помощью программы restrick.exe?
7. В чем недостаточность средств ограничения прав пользователей, предоставляемых программой restrick.exe?
8. Как может быть заблокирована рабочая станция на период временного отсутствия пользователя? Укажите несколько вариантов.
9. Какой из способов блокирования рабочей станции на период временного отсутствия пользователя является наиболее безопасным и почему?
10. Как устанавливается защита от чтения документов Microsoft Word и таблиц Microsoft Excel?
11. Как реализована (в чем выражается) защита документов Microsoft Office от чтения с помощью паролей?
12. Насколько надежна защита документов Microsoft Office от чтения с помощью паролей?
13. Как устанавливается защита от изменения документов Microsoft Word и таблиц Microsoft Excel?
14. Как реализована (в чем выражается) защита документов Microsoft Office от изменения с помощью паролей?
15. Насколько надежна защита документов Microsoft Office от изменения с помощью паролей?
16. Как создать новую базу данных паролей с помощью программы whisper.exe и защитить ее от несанкционированного доступа?
17. Как реализована (в чем выражается) защита базы данных паролей программы whisper.exe?
18. Как добавить новый пароль в базу данных программы whisper.exe?
19. Какая информация указывается при добавлении новой записи в базу данных программы whisper.exe?
20. Для чего в программе whisper.exe предназначена функция Generate?
21. Для чего предназначены элементы управления в окне автоматической генерации паролей программы whisper.exe?

22. Как скрыть отображаемые на экране пароли из базы данных программы whisper.exe, но при этом сохранить возможность их переноса в требуемую программу?
23. Какие права доступа к личным и разделяемым файлам и папкам устанавливаются операционной системой по умолчанию?
24. Кто может управлять разрешениями на доступ к ресурсу?
25. Какая информация содержится в дескрипторе безопасности объекта?
26. Какая модель разграничения доступа к объектам реализована в защищенных версиях операционной системы Windows?
27. В чем основные недостатки модели разграничения доступа к объектам, реализованной в защищенных версиях операционной системы Windows?
28. Какие специфические права доступа могут быть определены для принтера?
29. Какие специфические права доступа могут быть определены для раздела реестра?
30. Какие разрешения на доступ к принтеру установлены в системе и почему?
31. Какие установлены разрешения на доступ к разделу реестра HKEY_LOCAL_MACHINE и почему?
32. Какие установлены разрешения на доступ к разделам реестра HKEY_CURRENT_USER и HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies и почему?
33. Кто управляет разрешениями на доступ к принтерам и почему?
34. Кто управляет разрешениями на доступ к разделам реестра и почему?
35. Какие из объектов могут наследовать разрешения на доступ к ним и от кого?
36. Для чего предназначены параметры создаваемой учетной записи пользователя?
37. В чем разница между отключением и блокировкой учетной записи?
38. В чем целесообразность разбиения множества пользователей на группы?
39. Как назначаются права пользователям и группам в защищенных версиях операционной системы Windows?
40. Какие требования по сложности могут предъявляться к паролям в операционной системе Windows?
41. Для чего предназначены параметры парольной аутентификации, связанные с установкой минимального срока действия и неповторяемости паролей?
42. Какие параметры могут быть установлены для политики блокировки учетных записей?
43. Для чего предназначены параметры политики блокировки учетных записей?
44. В чем слабость парольной аутентификации?
45. Как может быть повышена надежность аутентификации с помощью паролей?
46. Какой может быть реакция системы на попытку подбора паролей?
47. Кому может быть разрешен доступ по чтению ко всей базе учетных записей пользователей и почему?

48. Кому может быть разрешен доступ по записи к базе учетных записей пользователей и почему?

Варианты для выбора номеров контрольных вопросов

№	Номера вопросов	№	Номера вопросов	№	Номера вопросов
1	1, 2, 9, 18, 32, 35	11	4, 13, 23, 29, 41, 48	21	1, 8, 16, 28, 38, 48
2	3, 10, 11, 19, 34, 36	12	16, 24, 28, 33, 38, 43	22	2, 17, 25, 27, 32, 35
3	4, 12, 20, 21, 37, 43	13	8, 15, 23, 27, 36, 37	23	3, 11, 13, 18, 36, 38
4	5, 13, 22, 27, 38, 44	14	7, 14, 20, 22, 34, 35	24	4, 14, 24, 30, 34, 44
5	6, 14, 23, 28, 39, 45	15	2, 12, 21, 31, 32, 44	25	5, 15, 20, 25, 35, 40
6	7, 15, 24, 29, 40, 46	16	3, 15, 20, 25, 39, 45	26	6, 16, 26, 31, 36, 42
7	8, 16, 25, 30, 41, 47	17	4, 9, 26, 27, 32, 47	27	7, 11,17, 27, 37, 47
8	17, 26, 31, 33, 42, 48	18	5, 10, 19, 22, 37, 46	28	8, 9, 18, 22, 38, 43
9	2, 10, 21, 27, 39, 46	19	6, 16, 26, 30, 40, 48	29	1, 10, 19, 33, 41, 45
10	3, 12, 22, 28, 40, 47	20	10, 11, 20, 32, 33, 43	30	2, 11, 17, 30, 37, 46

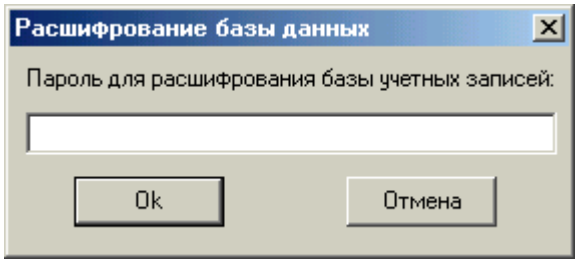
Лабораторная работа 7. Использование функций криптографического интерфейса Windows для защиты информации

Содержание задания

1. В программу, разработанную при выполнении лабораторной работы № 1, добавить средства защиты от несанкционированного доступа к файлу с учетными данными зарегистрированных пользователей.
2. Файл с учетными данными должен быть зашифрован при помощи функций криптографического интерфейса операционной системы Windows (CryptoAPI) с использованием сеансового ключа, генерируемого на основе вводимой администратором (пользователем) парольной фразы.
3. При запуске программы файл с учетными данными должен расшифровываться во временный файл (или в файл в оперативной памяти), который после завершения работы программы должен быть снова зашифрован для отражения возможных изменений в учетных записях пользователей. «Старое» содержимое файла учетных записей при этом стирается.
4. После ввода парольной фразы при запуске программы, генерации ключа расшифрования и расшифрования файла с учетными данными зарегистрированных пользователей правильность введенной парольной фразы определяется по наличию в расшифрованном файле учетной записи администратора программы.
5. При вводе неправильной парольной фразы или отказе от ее ввода работа программы должна завершаться с выдачей соответствующего сообщения.
6. Временный файл на диске с расшифрованными учетными данными после завершения работы программы удаляется.
7. Варианты использования алгоритмов шифрования и хеширования выбираются в соответствии с выданным преподавателем заданием.
8. Для доступа к функциям CryptoAPI из программ на Паскале следует использовать интерфейсный модуль wincrypt.pas с указанного преподавателем сетевого диска.

Возможный вид дополнительных диалоговых форм программы

Окно запроса парольной фразы для расшифровки файла с учетными данными



Может быть создано на основе шаблона Password Dialog, выбираемого с помощью команды File | New | Dialogs систем программирования Borland Delphi или Borland C++ Builder. Для повышения безопасности эта форма должна быть исключена из списка автоматически создаваемых форм проекта (команда Project | Options | Forms) и создаваться (уничтожаться) в программе явным образом.

Индивидуальные варианты заданий

№	Тип симметричного шифрования	Используемый режим шифрования	Добавление к ключу случайного значения	Используемый алгоритм хеширования
1	2	3	4	5
1	Блочный	Электронная кодовая книга	Да	MD2
2	Потоковый	-	Да	MD2
3	Блочный	Сцепление блоков шифра	Да	MD2
4	Потоковый	-	Да	MD5
5	Блочный	Обратная связь по шифротексту	Да	MD2
6	Потоковый	-	Да	SHA
7	Блочный	Электронная кодовая книга	Да	MD4
1	2	3	4	5
8	Потоковый	-	Нет	MD2
9	Блочный	Сцепление блоков шифра	Да	MD4
10	Потоковый	-	Нет	MD5
11	Блочный	Обратная связь по шифротексту	Да	MD4
12	Потоковый	-	Нет	SHA
13	Блочный	Электронная кодовая книга	Да	MD5
14	Блочный	Сцепление блоков шифра	Да	MD5
15	Блочный	Обратная связь по шифротексту	Да	MD5
16	Блочный	Электронная кодовая книга	Да	SHA
17	Блочный	Сцепление блоков шифра	Да	SHA
18	Блочный	Обратная связь по шифротексту	Да	SHA
19	Блочный	Электронная кодовая книга	Нет	MD2
20	Блочный	Сцепление блоков шифра	Нет	MD2
21	Блочный	Обратная связь по шифротексту	Нет	MD2
22	Блочный	Электронная кодовая книга	Нет	MD4
23	Блочный	Сцепление блоков шифра	Нет	MD4
24	Блочный	Обратная связь по шифротексту	Нет	MD4

25	Блочный	Электронная кодовая книга	Нет	MD5
26	Блочный	Сцепление блоков шифра	Нет	MD5
27	Блочный	Обратная связь по шифро-тексту	Нет	MD5
28	Блочный	Электронная кодовая книга	Нет	SHA
29	Блочный	Сцепление блоков шифра	Нет	SHA
30	Блочный	Обратная связь по шифро-тексту	Нет	SHA

5. ПЕРЕЧЕНЬ ПРОГРАММНЫХ ПРОДУКТОВ, ИСПОЛЬЗУЕМЫХ В ПРЕПОДАВАНИИ ДИСЦИПЛИНЫ «МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»

Лекции проводятся в стандартной аудитории, оснащенной в соответствии с требованиями преподавания теоретических дисциплин.

Для проведения лабораторных работ необходим компьютерный класс на 12-14 посадочных рабочих мест пользователей. В классе должны быть установлены языки программирования Си++, PacaL

6. ФОНД ТЕСТОВЫХ И КОНТРОЛЬНЫХ ЗАДАНИЙ ДЛЯ ОЦЕНКИ КАЧЕСТВА ЗНАНИЙ СТУДЕНТОВ

Контрольный тест

1. Меры информационной безопасности направлены на защиту от:

- нанесения неприемлемого ущерба
- нанесение любого ущерба
- нанесение ущерба

2. Перехват данных является угрозой:

- Доступности
- Конфиденциальности
- Целостности

3. В следующих странах сохранилось жесткое государственное регулирование разработки и распространения криптосредств на внутреннем рынке:

- Китай
- Россия
- Франция

4. Уровень безопасности А, согласно «Оранжевой книге», характеризуется:

- Произвольным управлением доступом
- Принудительным управлением доступом
- Верифицируемой безопасностью

5. В число целей политики безопасности верхнего уровня входят:

- Формулировка целей, которые преследует организация в области информационной безопасности
- Определение правил разграничения доступа
- Определение общих направлений в достижении целей безопасности

6. Риск является функцией:

- размера возможного ущерба
- числа уязвимых мест в системе
- уставного капитала организации

7. В число классов мер процедурного уровня входят:

- управление персоналом
- управление персоналками
- реагирование на нарушения режима безопасности

8. Укажите наиболее существенные с точки зрения безопасности особенности современных российских ИС:

- использование ПО с активными агентами
- использование пиратского ПО
- использование свободно распространяемого ПО

9. В число основных понятий ролевого управления доступом входят:

- объект
- субъект
- метод

10. Пороговый метод выявления атак хорош тем, что он:

- поднимает мало ложных тревог
- способен обнаруживать неизвестные атаки
- прост в настройке и эксплуатации

11. Российский и американский стандарты шифрования основаны на классе шифров:

- шифры гаммирования
- блочные шифры
- шифры перестановки

12. Разборчивость бывает:

- словесная
- логическая
- сетевая

13. Принцип усиления самого слабого звена можно переформулировать как:

- принцип равнопрочности обороны
- принцип удаления слабого звена
- принцип выявления главного звена

14. Согласно рекомендациям X.800, аутентификация может быть реализована на:

- Сетевом уровне
- Транспортном уровне
- Прикладном уровне

15. В число возможных стратегий нейтрализации рисков входят:

- переадресация риска
- деноминация риска
- декомпозиция риска

16. Агрессивное потребление ресурсов является угрозой:

- Доступности
- Конфиденциальности
- Целостности

17. По мере возникновения угрозы могут быть:

- вероятная
- невероятная
- успешная

18. Основным лицензирующим органом в области защиты информации является:

- совет Федерации
- Гостехкомиссия России
- Министерство связи

19. Разглашение – это _____

20. Целостность – это _____

7. КОМПЛЕКТ ЭКЗАМЕНАЦИОННЫХ БИЛЕТОВ

Экзаменационные билеты для студентов включают один теоретический вопрос и задачу. Вопросы к экзамену выдаются студентам на последней лекции. Задачи, включаемые в экзаменационный билет аналогичны задачам, которые выполнялись в течение семестра. Примерный комплект экзаменационных билетов выглядит следующим образом.

АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Утверждено на заседании кафедры
_____
Заведующий кафедрой
Утверждаю:_____

Кафедра___ИУС___
Факультет___МиИ_
Курс __4_____
Дисциплина_ЗИ__

Экзаменационный билет №__1___

1. Управление рисками. Основные понятия, принципы, этапы..
2. Система ЭЦП.

АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Утверждено на заседании кафедры
_____
Заведующий кафедрой
Утверждаю:_____

Кафедра___ИУС___
Факультет___МиИ_
Курс __4_____
Дисциплина_ЗИ__

Экзаменационный билет №__2___

1. Значение и роль ИБ в современном мире.
2. Критерии классификации угроз.

АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Утверждено на заседании кафедры
_____
Заведующий кафедрой
Утверждаю:_____

Кафедра___ИУС___
Факультет___МиИ_
Курс __4_____
Дисциплина_ЗИ__

Экзаменационный билет №__3___

1. Основные механизмы и сервисы безопасности.
2. Программно-технические меры обеспечения ИБ, виды, архитектурные принципы, сервисы.

8. КАРТА ОБЕСПЕЧЕННОСТИ ДИСЦИПЛИНЫ КАДРАМИ ПРОФЕССОРСКО – ПРЕПОДАВАТЕЛЬСКОГО СОСТАВА

№	Наименование дисциплин в соответствии с учебным планом	Обеспеченность преподавательским составом								
		Ф.И.О. должность по штатному расписанию	Какое образовательное учреждение профессионального образования окончил, специальность по диплому	Ученая степень и ученое звание	Стаж научно педагогической работы			Основное место работы, должность	Условия привлечения к трудовой деятельности (штатный, совместитель, внутренний или внешний с указанием доли ставки), иное	Кол-во часов
					Всего	В т. ч. педагогический				
						Всего	В том числе по преподаваемой дисциплине			
	Методы и средства защиты компьютерной информации	Самохвалова С.Г.	ДВГУ, математик	доцент, к.т.н.	19	18	2	АмГУ, каф. ИУС	Штатный	129

i

ii

iii