Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Амурский государственный университет»

Кафедра Информационных и управляющих систем

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Основной образовательной программы по специальности 230201.65 –
Информационные систем и технологии

Благовещенск 2011

УМКД разработан _____
(степень, звание, фамилия, имя, отчество разработчиков)

_____

_____

Рассмотрен и рекомендован на заседании кафедры

Протокол заседания кафедры от «____» _____ 20___ г. № _____

Зав. кафедрой _____ /_____ /
(подпись) (И.О. Фамилия)

УТВЕРЖДЕН

Протокол заседания УМСФ _____
(указывается название факультета по принадлежности специальности)

от _____ № _____

Председатель УМСФ _____ /_____ /
(подпись) (фамилия, имя, отчество)

СОДЕРЖАНИЕ

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
«Амурский государственный университет»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ В.В. Проказин
«_____» _____ 2011г.

РАБОЧАЯ ПРОГРАММА

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Специальность 230201.65 Информационные систем и технологии
Квалификация (степень) выпускника инженер

Курс 5 Семестр 9

Лекции 28 (час.) Экзамен 9

Лабораторные занятия 38 (час.)
Самостоятельная работа 70 (час.)
Общая трудоемкость дисциплины 136 (час.)

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

Факультет математики и информатики
Кафедра информационных и управляющих систем

2011г.

Рабочая программа составлена на основании Государственного образовательного стандарта высшего профессионального образования для специальности 230201.65 – Информационные системы и технологии

Рабочая программа обсуждена на заседании кафедры информационных и управляющих систем
«__» _____20____ г., протокол № _____
Заведующий кафедрой _____

Рабочая программа одобрена на заседании учебно-методического совета специальности 230201.65 Информационные системы и технологии

«____» _____20___ г., протокол № _____

Председатель _____

Рабочая программа переутверждена на заседании кафедры от _____протокол № ___

Зав.кафедрой _____ _____

СОГЛАСОВАНО
Начальник учебно-методического управления

_____

«__» _____20___ г.

СОГЛАСОВАНО
Председатель учебно-методического совета факультета

_____ С.Г. Самохвалова

«__» _____20___ г.

СОГЛАСОВАНО
Заведующий выпускающей кафедрой

_____ А.В. Бушманов

«__» _____20___ г.

СОГЛАСОВАНО
Директор научной библиотеки

_____ Л.А. Проказина

«__» _____20___ г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью преподавания дисциплины является ознакомление с общей проблемой информационной безопасности информационных систем, организационными, техническими и другими методами и средствами защиты информации, с законодательством и стандартами в этой области, с современными криптосистемами, с компьютерными средствами реализации защиты в информационных системах, изучение методов идентификации пользователей, борьбы с вирусами.

В результате изучения программы курса студенты должны:

знать правовые основы защиты компьютерной информации, организационные, технические и программные методы защиты информации в ИС, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов;

уметь применять методы защиты компьютерной информации;

иметь представление о направлениях развития и перспективах защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

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

Знания, умения и навыки, полученные в процессе изучения данного курса, могут быть использованы студентами при выполнении выпускной квалификационной работы.

3.СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 129 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости Форма промежуточной аттестации
				лек	лаб	пр	сам.	
1	Введение. Понятие информационной безопасности. Основные составляющие.	9	1-2	5				
2	Наиболее распространенные угрозы	9	3-4	4			4	тест
3	Законодательный уровень информационной безопасности	9	4-5	4			6	тест
4	Стандарты и спецификации в области информационной безопасности	9	5-7	6			6	контрольная работа
5	Административный уровень информационной безопасности. Управление рисками.	9	7-9	6			6	тест
6	Процедурный уровень информационной безопасности	9	9-10	4	5		6	контрольная работа
7	Основные программно-технические меры	9	11-12	4	10		6	тест
8	Идентификация и аутентификация, управление доступом	9	13	2	5		6	тест

9	Протоколирование и аудит, шифрование, контроль целостности	9	13-14	6	10		8	тест
10	Экранирование, анализ защищенности. Обеспечение высокой доступности	9	15	4			6	тест

4. СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ

4.1. Лекции

Тема 1. Введение. Понятие информационной безопасности. Основные составляющие.

Предмет защиты. Виды и формы представления информации. Понятие информационной безопасности. Основные составляющие информационную безопасность.

Тема 2. Наиболее распространенные угрозы.

Основные определения и критерии классификации угроз. Случайные угрозы. Преднамеренные угрозы. Вредоносное программное обеспечение. Основные угрозы целостности, доступности, конфиденциальности.

Тема 3. **Законодательный уровень информационной безопасности**

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

Тема 4. Стандарты и спецификации в области информационной безопасности

Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Рекомендации X.800. Стандарт «Критерии оценки безопасности информационных технологий». Руководящие документы Гостехкомиссии России.

Тема 5. Административный уровень информационной безопасности. Управление рисками.

Основные понятия. Политика безопасности. Программа безопасности. Подготовительные этапы управления рисками. Основные этапы управления рисками.

Тема 6. Процедурный уровень информационной безопасности

Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ..

Тема 7. **Основные программно-технические меры**

Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность.

Тема 8. Идентификация и аутентификация, управление доступом

Основные понятия. Парольная аутентификация. Одноразовые пароли. Идентификация/аутентификация с помощью биометрических данных. Ролевое управление доступом.

Тема 9. Протоколирование и аудит, шифрование, контроль целостности

Основные понятия. Активный аудит. Функциональные компоненты и архитектура. Цифровые сертификаты.

Тема 10. Экранирование, анализ защищенности. Обеспечение высокой доступности

Основные понятия. Архитектурные аспекты. Классификация межсетевых экранов. Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости и обслуживаемости.

4.2. Лабораторные занятия

Лабораторная работа 1. Оценочный расчет защищенности помещений от утечки речевых сообщений по акустическому каналу.

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

Лабораторная работа 3. Изучение традиционных симметричных криптосистем. Шифры перестановок.

Лабораторная работа 4. Изучение традиционных симметричных криптосистем Шифры замены.

Лабораторная работа 5. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации.

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

5. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	№ раздела (темы) дисциплины	Форма (вид) самостоятельной работы	Трудоёмкость в часах
1	Введение. Понятие информационной безопасности. Основные составляющие.		
2	Наиболее распространенные угрозы	Работа с лекционным материалом	4
3	Законодательный уровень информационной безопасности	Подготовка к лабораторным работам, подготовка к тесту	6
4	Стандарты и спецификации в области информационной безопасности	Работа с лекционным материалом. Подготовка к контрольной работе	6
5	Административный уровень информационной безопасности. Управление рисками.	Работа с лекционным материалом. Подготовка к лабораторным работам, подготовка к тесту	6
6	Процедурный уровень информационной безопасности	Подготовка к лабораторным работам, подготовка к тесту	6
7	Основные программно-технические меры	Работа с лекционным материалом. Подготовка к лабораторным работам, выполнение домашних заданий, подготовка к тесту	6
8	Идентификация и аутентификация, управление доступом	Работа с лекционным материалом. Подготовка к лабораторным работам, выполнение домашних заданий, подготовка к тесту	6
9	Протоколирование и аудит, шифрование, контроль целостности	Работа с лекционным материалом. Подготовка к лабораторным работам, выполнение домашних заданий, подготовка к тесту	8
10	Экранирование, анализ защищенности. Обеспечение высокой доступности	Работа с лекционным материалом. Подготовка к лабораторным работам, выполнение домашних заданий, подготовка к тесту	6

Содержание самостоятельной работы студентов по дисциплине

Изучение материала дисциплины по конспекту лекций, учебным и справочным пособиям, методическим пособиям при подготовке к лабораторным занятиям.

Оформление отчетов о лабораторных работах

В процессе изучения дисциплины студенты должны самостоятельно овладеть следующими темами:

1. Статистический анализ каналов связи.
2. Критерий Манна - Уитни. Критерий Уилкоксона.

3. Критерий знаков для анализа парных повторных наблюдений.
4. Анализ повторных парных наблюдений с помощью знаковых рангов.
5. Арифметическое кодирование.
6. Арифметический вес. Арифметическое расстояние.
7. Условие обнаружения ошибок. Условие исправления ошибок.
8. Коды с обнаружением ошибок.
9. Коды с исправлением одиночных ошибок.

6.ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Результаты освоения дисциплины достигаются за счет использования в процессе обучения современных инструментальных средств: лекции с применением мультимедийнных технологий.

При проведении занятий используются активные и интерактивные формы: методы IT; работа в команде; проблемное обучение, контекстное обучение, междисциплинарное обучение, опережающая самостоятельная работа

7.ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Для организации текущего контроля полученных студентами знаний по данной дисциплине используются тесты. Каждый тест имеет 1 вариант ответа и содержит несколько вопросов. Текущий контроль освоения дисциплины осуществляется на лабораторных занятиях. Экзаменационные билеты также содержат теоретическую часть.

Примерные вопросы к экзамену

1. Понятие ИБ. Основные составляющие ИБ и их роль при создании ИС.
2. Значение и роль ИБ в современном мире.
3. Угрозы ИБ (основные определения) и критерии классификации угроз.
4. Примеры угроз и рисков по всем основным составляющим (аспектам) ИБ.
5. Анализ угроз и рисков ИС с точки зрения ИБ.
6. Российское и международное законодательство в области защиты информации.
7. Стандарты и спецификации в области защиты информации, их основные положения и принципы построения.
8. «Оранжевая книга» как оценочный стандарт.
9. Критерии оценки безопасности информационных технологий
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.
20. Использование криптографических технологий в ИС.
21. Технические средства, обеспечивающие защиту информации, их классификация и назначение.
22. Реагирование на нарушение режима безопасности, процедуры плановых восстановительных работ.

23. Особенности современных информационных систем, существенные с точки зрения безопасности.

24. Ролевое управление доступом.

25. Активный и пассивный аудит.

Образец тестовых заданий

1. Основными составляющими информационной безопасности являются

а) конфиденциальность, целостность, доступность

б) глубина, достоверность, адекватность

в) своевременность, актуальность, полнота

2. Величина угрозы для элемента информации определяется как

а) произведение ущерба от реализации угрозы и вероятности ее реализации

б) сумма ущерба от реализации угрозы и вероятности ее реализации

в) определить невозможно

3. Происхождение термина «криптография» :

а) от слова «тайнопись»;

б) от слова «шифрование»;

в) от термина «кодирование»;

4. Метод надежной передачи информации по открытому каналу связи использует:

а) криптографию;

б) стеганографию;

в) кодирование;

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) **основная литература**

1. Романов, О. А. Организационное обеспечение информационной безопасности: учеб. пособие: рек. УМО / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 190 с.

2. Ярочкин, В. И. Информационная безопасность : учеб. : рек. Мин. обр. РФ / В. И. Ярочкин. - 5-е изд. - М. : Академический Проект, 2008. - 544 с.

3. Грибунин, В. Г. Комплексная система защиты информации на предприятии : учеб. пособие : рек. УМО / В. Г. Грибунин, В. В. Чудовский. - М. : Академия, 2009. - 413 с.

4. Расторгуев, С. П. Основы информационной безопасности: учеб. пособие: рек. УМО / С. П. Расторгуев. - М. : Академия, 2007. - 188 с.

5. Родичев, Ю. А. Информационная безопасность и защита информации: учеб. пособие / Ю. М. Краковский. - М. ; Ростов н/Д : Март, 2008. - 288 с.

б) **дополнительная литература**

1. Куприянов, А. И. Основы защиты информации: учеб. пособие: рек. УМО / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - М. : Академия, 2006. - 255 с.

2. Галатенко, В. А. Основы информационной безопасности: курс лекций: Доп. УМО в обл. прикладной информ. / В.А. Галатенко; Под ред. В.Б. Бетелин. - М. : Интернет-Ун-т Информ. Технологий, 2003. - 279 с.

3. Мельников, В. П. Информационная безопасность: учеб. пособие: рек. Мин. обр. РФ / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - М. : Академия, 2005. - 333 с.

4. Информационная безопасность: нормативно-правовые аспекты: учеб. пособие : рек. УМО / Ю. А. Родичев. - М. : Питер, 2008. - 271 с.

в) **периодические издания**

Информационные технологии и вычислительные системы

Проблемы передачи информации

Черные дыры в Российском законодательстве

г) **Интернет-ресурсы**

№	Наименование ресурса	Краткая характеристика
1	http://www.iqlib.ru	Интернет-библиотека образовательных изданий, в которой собраны электронные учебники, справочные и учебные пособия. Удобный поиск по ключевым словам, отдельным темам и отраслям знания
2	http://www.intuit.ru/	Интернет университет информационных технологи, содержит бесплатные учебные курсы, учебники и методические пособия по всем направлениям подготовки
3	http://www.itsec.ru	Электронный журнал по информационной безопасности.

9.МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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.

2. КОНСПЕКТ ЛЕКЦИЙ ПО ДИСЦИПЛИНЕ

Тема 1. Введение. Понятие информационной безопасности. Основные составляющие.

Понятие «информация» сегодня употребляется весьма широко и разносторонне. Трудно найти такую область знаний, где бы оно не использовалось. Огромные информационные потоки буквально захлестывают людей. Объем научных знаний, например, но оценке специалистов, удваивается каждые пять лет.

Как и всякий продукт, информация имеет потребителей, нуждающихся в ней, и потому обладает определенными потребительскими качествами, а также имеет и своих обладателей или производителей.

С точки зрения потребителя, качество используемой информации позволяет получать дополнительный экономический или моральный эффект.

С точки зрения обладателя — сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства и сбыта товаров и услуг. Это, естественно, требует определенных действий, направленных на защиту конфиденциальной информации.

Понимая под безопасностью состояние защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз, можно выделить и компоненты безопасности — такие, как персонал, материальные и финансовые средства и информацию. Анализ состояния дел в сфере защиты информации показывает, что уже сложилась вполне сформировавшаяся концепция и структура защиты, основу которой составляю весьма развитый арсенал технических средств защиты информации, производимых на промышленной основе;

- значительное число фирм, специализирующихся на решении вопросов защиты информации;
- достаточно четко очерченная система взглядов на эту проблему;
- наличие значительного практического опыта и другое.

И тем не менее, как свидетельствует отечественная и зарубежная печать, злоумышленные действия над информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту.

Опыт показывает, что для борьбы с этой тенденцией необходима стройная и целенаправленная организация процесса защиты информационных ресурсов. Причем в этом должны активно участвовать профессиональные специалисты, администрация, сотрудни-

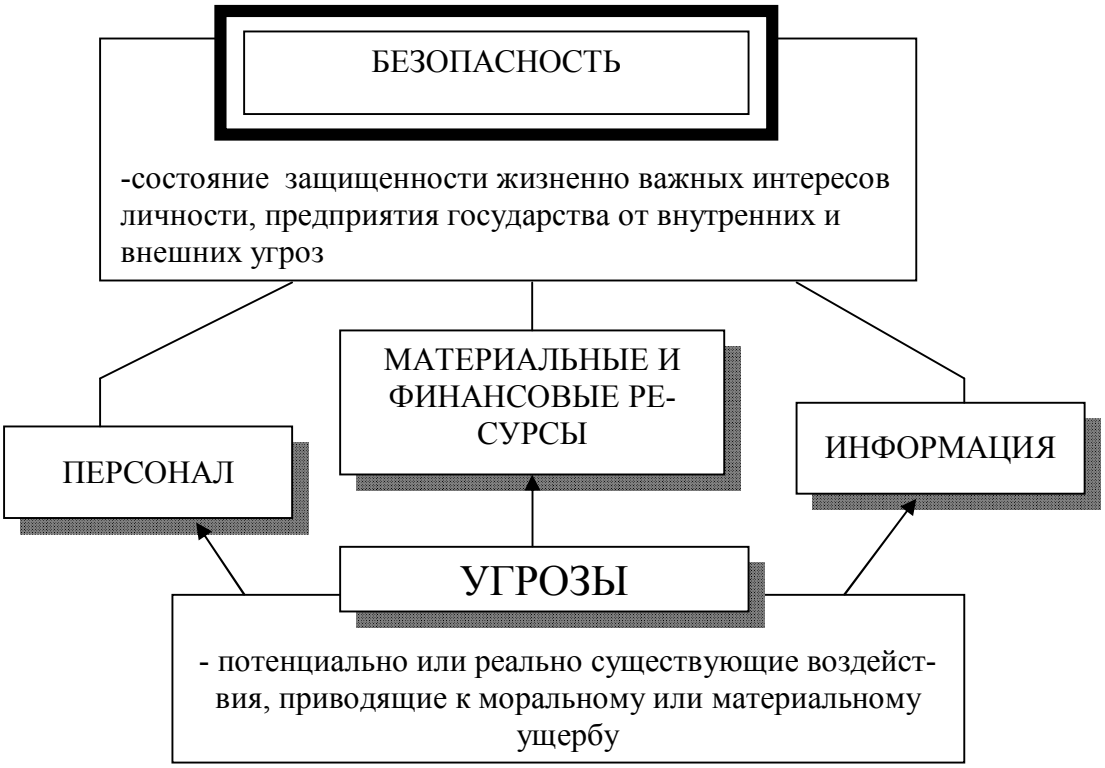
ки и пользователи, что и определяет повышенную значимость организационной стороны вопроса.

Опыт также показывает, что:

• обеспечение безопасности информации не может быть одноразовым актом. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий;

• безопасность информации может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты во всех структурных элементах производственной системы и на всех этапах технологического цикла обработки информации. Наибольший эффект достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм — систему защиты информации (СЗИ). При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий;

• никакая СЗИ не может обеспечить требуемого уровня безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех установленных правил, направленных на ее защиту



С учетом накопленного опыта можно определить систему защиты информации как организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

С позиций системного подхода к защите информации предъявляются определенные требования. Защита информации должна быть:

• непрерывной. Это требование проистекает из того, что злоумышленники только и ищут возможность, как бы обойти защиту интересующей их информации;

• плановой. Планирование осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели предприятия (организации);

• целенаправленной. Защищается то, что должно защищаться в интересах конкретной цели, а не все подряд;

• конкретной. Защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;

• активной. Защищать информацию необходимо с достаточной степенью настойчивости;

• надежной. Методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам, независимо от формы их представления, языка выражения и вида физического носителя, на котором они закреплены;

• универсальной. Считается, что в зависимости от вида канала утечки или способа несанкционированного доступа его необходимо перекрывать, где бы он ни проявился, разумными и достаточными средствами, независимо от характера, формы и вида информации;

• комплексной. Для защиты информации во всем многообразии структурных элементов должны применяться все виды и формы защиты в полном объеме. Недопустимо применять лишь отдельные формы или технические средства. Комплексный характер защиты проистекает из того, что защита — это специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов.

К системе безопасности информации предъявляются также определенные требования:

• четкость определения полномочий и прав пользователей на доступ к определенным видам информации;

• предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы;

• сведение к минимуму числа общих для нескольких пользователей средств защиты;

• учет случаев и попыток несанкционированного доступа к конфиденциальной информации;

• обеспечение оценки степени конфиденциальной информации;

• обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя.

Система защиты информации, как любая система, должна иметь определенные виды собственного обеспечения, опираясь на которые она будет выполнять свою целевую функцию. С учетом этого СЗИ может иметь:

• правовое обеспечение. Сюда входят нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действия;

• организационное обеспечение. Имеется в виду, что реализация защиты информации осуществляется определенными структурными единицами, такими как: служба защиты документов; служба режима, допуска, охраны; служба защиты информации техническими средствами; информационно-аналитическая деятельность и другими;

• аппаратное обеспечение. Предполагается широкое использование технических средств как для защиты информации, так и для обеспечения деятельности собственно СЗИ;

• информационное обеспечение. Оно включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы. Сюда могут входить как показатели доступа, учета, хранения, так и системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности;

• программное обеспечение. К нему относятся различные информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и путей несанкционированного проникновения к источникам конфиденциальной информации;

• математическое обеспечение. Предполагает использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты;

• лингвистическое обеспечение. Совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;

• нормативно-методическое обеспечение. Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации, различного

рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации.

Как и любая система, система информационной безопасности имеет свои цели, задачи, методы и средства деятельности, которые согласовываются по месту и времени в зависимости от условий.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

Доступность — это возможность за приемлемое время получить требуемую информационную услугу.

Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность - это защита от несанкционированного доступа к информации.

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Конфиденциальность - самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Тема 2. Наиболее распространенные угрозы

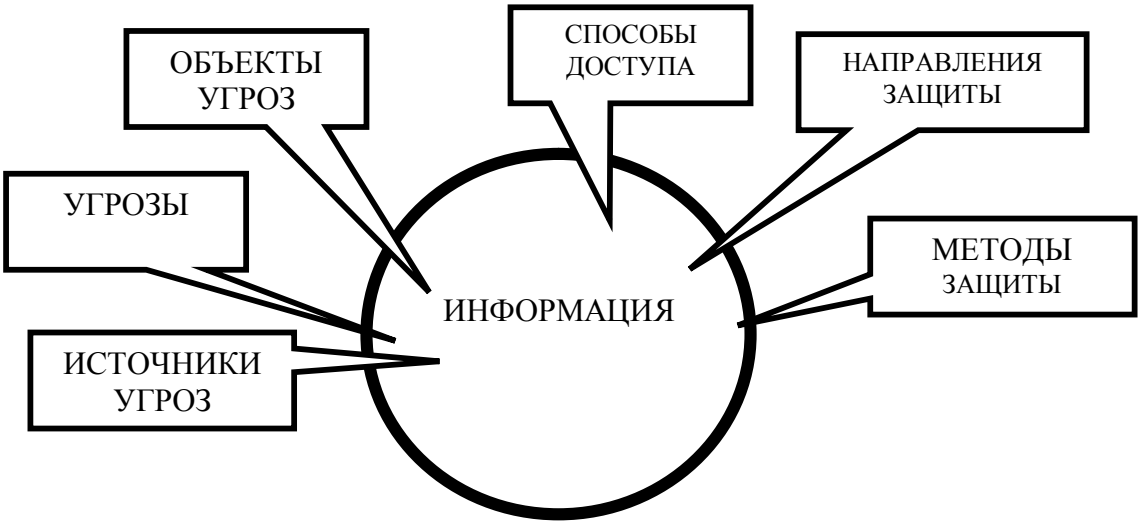
Понимая информационную безопасность как «состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций», правомерно определить угрозы безопасности информации, источники этих угроз, способы их реализации и цели, а также иные условия и действия, нарушающие безопасность.

Под угрозами конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями.

Такими действиями являются:

- ознакомление с конфиденциальной информацией различными путями и способами без нарушения ее целостности;
- модификация информации в криминальных целях как частичное или значительное изменение состава и содержания сведений;
- разрушение (уничтожение) информации как акт вандализма с целью прямого нанесения материального ущерба,

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

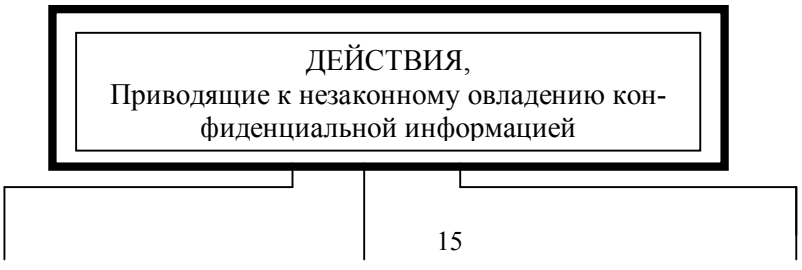


В конечном итоге противоправные действия с информацией приводят к нарушению ее конфиденциальности, полноты, достоверности и доступности, что в свою очередь приводит к нарушению как режима управления, так и его качества в условиях ложной или неполной информации.

Отношение объекта (фирма, организация) и субъекта (конкурент, злоумышленник) в информационном процессе с противоположными интересами можно рассматривать с позиции активности в действиях, приводящих к овладению конфиденциальными сведениями. В этом случае возможны такие ситуации:

- владелец (источник) не принимает никаких мер к сохранению конфиденциальной информации, что позволяет злоумышленнику легко получить интересующие его сведения;
- источник информации строго соблюдает меры информационной безопасности, тогда злоумышленнику приходится прилагать значительные усилия к осуществлению доступа к охраняемым сведениям, используя для этого всю совокупность способов несанкционированного проникновения: легальное или нелегальное;
- промежуточная ситуация — это утечка информации по техническим каналам, при которой источник еще не знает об этом (иначе он принял бы меры защиты), а злоумышленник легко, без особых усилий может их использовать в своих интересах.

В общем факт получения охраняемых сведений злоумышленниками или конкурентами называют утечкой. Однако одновременно с этим в значительной части законодательных актов, законов, кодексов, официальных материалов используются и такие понятия, как разглашение сведений и несанкционированный доступ к конфиденциальной информации.



1. Разглашение — это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним.

2. Утечка — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

3. Несанкционированный доступ — это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам.

Если исходить из комплексного подхода к обеспечению информационной безопасности, то такое деление ориентирует на защиту информации как от разглашения, так и от утечки по техническим каналам и от несанкционированного доступа к ней со стороны конкурентов и злоумышленников.

Такой подход к классификации действий, способствующих неправомерному овладению конфиденциальной информацией, показывает многогранность угроз и многоаспектность защитных мероприятий, необходимых для обеспечения комплексной информационной безопасности.

Условия способствующие неправомерному овладению конфиденциальной информацией следующие:

• разглашение (излишняя болтливость сотрудников) — 32%;

• несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок — 24%;

• отсутствие на фирме надлежащего контроля и жестких условий обеспечения информационной безопасности—14%;

• традиционный обмен производственным опытом — 12%;

• бесконтрольное использование информационных систем — 10%;

• наличие предпосылок возникновения среди сотрудников конфликтных ситуаций — 8%.

Среди форм и методов недобросовестной конкуренции находят наибольшее распространение:

• экономическое подавление, выражающееся в срыве сделок и иных соглашений (48%), парализации деятельности фирмы (31%), компрометации фирмы (11%), шантаже руководителей фирмы (10%);

• физическое подавление: ограбления и разбойные нападения на офисы, склады, грузы (73%), угрозы физической расправы над руководителями фирмы и ведущими специалистами (22%), убийства и захват заложников (5%);

• информационное воздействие: подкуп сотрудников (43%), копирование информации (24%), проникновение в базы данных (18%), продажа конфиденциальных документов (10%), подслушивание телефонных переговоров и переговоров в помещениях (5%), а также ограничение доступа к информации, дезинформация;

• финансовое подавление включает такие понятия, как инфляция, бюджетный дефицит, коррупция, хищение финансов, мошенничество;

• психическое давление может выражаться в виде хулиганских выходок, угрозы и шантажа, энергоинформационного воздействия.

Основные определения и критерии классификации угроз

Угроза — это потенциальная возможность определенным образом разрушить информационную безопасность. Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку - злоумышленником.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибка в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется называется окном опасности. Пока существует окно опасности, возможны успешные атаки.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда — недель), поскольку за это время должны произойти следующие события:

- должно стать известно о средствах использования пробела в защите;
- должны быть выпущены соответствующие заплаты;
- заплаты должны быть установлены в защищаемой ИС.

Новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат - как можно более оперативно.

Само понятие "угроза" в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать - вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений.

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Иногда такие ошибки и являются собственно угрозами (неправильно •веденные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь - следствие непреднамеренных ошибок.

Другие угрозы доступности классифицируем по компонентам ИС, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующую угрозу:

- нежелание работать с информационной системой (чаше всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);

- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.):

- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- нарушение работы (случайное или умышленное) систем сети, электропитания, водо- и/или теплоснабжения, кондиционирования:
- разрушение или повреждение помещений;

- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые "обиженные" сотрудники — нынешние и бывшие. Как правило, они стремятся нанести вред организации-"обидчику", например:

- испортить оборудование;
- встроить логическую бомбу, которая со временем разрушит программы и/или данные;
- удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Угрозы доступности могут выглядеть грубо — как повреждение или даже разрушение оборудования (в том числе носителей данных). Такое повреждение может вызываться естественными причинами. К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов, и случаи выгорания оборудования — не редкость.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители зачастую хранят небрежно, не обеспечивая их защиту от вредного воздействия окружающей среды. И когда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме — как скоординированные распределенные атаки, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание.

Для выведения систем из штатного режима эксплуатации могут использоваться уязвимые места в виде программных и аппаратных ошибок.

Вредоносное программное обеспечение

Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения. Выделим следующие грани вредоносного ПО:

- вредоносная функция;
- способ распространения;
- внешнее представление.

По механизму распространения различают:

- вирусы — код, обладающий способностью к распространении (возможно, с изменениями) путем внедрения в другие программы;
- "черви" — код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. "Черви", напротив, ориентированы в первую очередь на путешествия по сети.

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Вредоносный код, который выглядит как функционально полезная программа, называется троянским. Например, обычная программа, будучи пораженной вирусом, становится троянской; порой троянские программы изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке.

Для внедрения "бомб" часто используются ошибки типа "переполнение буфера", когда программа, работая с областью памяти, выходит за границы допустимого и записывает в нужные злоумышленнику места определенные данные.

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты.

С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

- ввести неверные данные;
- изменить данные.

Иногда изменяются содержательные данные, иногда — информация.

Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и программы. Внедрение рассмотренного выше вредоносного ПО - пример подобного нарушения.

Основные угрозы конфиденциальности

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно. Поскольку оно чревато получением несанкционированного доступа ко всей ИС.

Перехват данных — очень серьезная утром, и если конфиденциальность действительно является критичной, а данные пересылаются но многим каналам, их зашита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например па кабельную сеть, может кто угодно, так что эту угрозу нужно принимать, во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

К неприятным угрозам, от которых трудно защищаться, можно отнести и злоупотребление полномочиями. Таковы основные угрозы, которые наносит наибольший ущерб субъектам информационных отношений.

Тема 3. Законодательный уровень информационной безопасности

В деле обеспечения информационной безопасности успех может нести только комплексный подход. Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного;
- административного;
- процедурного;
- программно-технического.

Обзор российского законодательства в области ИБ

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.

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 фигурируют такие понятия, как банковская, коммерческая и служебная тайна.

Весьма продвинутым в плане информационной безопасности является Уголовный кодекс Российской Федерации (редакция от 2011 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"

Закон "Об информации, информационных технологиях и защите информации"

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информационных технологиях и защите информации" от 20 июня 2006 года. В нем даются основные определения и намечаются направления развития законодательства в данной области.

• **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.

Закон на первое место ставит сохранение конфиденциальности информации. Целостность представлена также достаточно хорошо, хотя и на втором месте. О доступности сказано довольно мало.

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. Защиту государственной тайны и персональных данных берет на себя государство; за другую конфиденциальную информацию отвечают ее собственники.

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".

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

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

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.

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.

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

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.

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, Феде-

ральное агентство правительственной связи и информации при Президенте Р Ф. Порядок выдачи сертификатов и лицензий устанавливается Правительством РФ.

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 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.

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

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...".

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 элек-

тронных 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.

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;
- ведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

Обзор зарубежного законодательства в области информационной безопасности

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.

За четыре года (1997-2001 гг.) на законодательном и других уровнях информационной безопасности США было сделано многое. Смягчены экспортные ограничения на криптосредства . Сформирована инфраструктура с открытыми ключами. Разработано большое число стандартов (например, новый стандарт электронной цифровой подписи P1P5 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 данном 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.

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 за-

щищенного 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. Стандарты и спецификации в области информационной безопасности.

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем». Данный труд, называемый чаще всего по цвету обложки "Оранжевой книгой", был впервые опубликован в августе 1983 года.

"Оранжевая книга" поясняет понятие безопасной системы, которая "управляет, с помощью соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию".

Очевидно, однако, что абсолютно безопасных систем не существует, это абстракция. Есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе.

В "Оранжевой книге" доверенная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

В рассматриваемых критериях и безопасность, и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности, целостности (статической). Вопросы доступности «Оранжевая книга» не затрагивает.

Важным средством обеспечения безопасности является механизм подотчетности (протоколирования). Доверенная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть анализом регистрационной информации.

Концепция доверенной вычислительной базы является центральной при оценке степени доверия безопасности. Доверенная вычислительная база — это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности, качество вычислительной базы определяется исключительно ее. реализацией и корректностью исходных данных, которые вводит системный администратор.

Основное назначение доверенной вычислительной базы выполнять функции монитора обращений, то есть контролировать допустимость выполнения Субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Монитор обращений должен обладать тремя качествами:

Изолированность. Необходимо предупредить возможность отслеживания работы монитора.

Полнота. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.

Верифицируемость. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Реализация монитора обращений называется ядром безопасности. Ядро безопасности — это основа, на которой строятся все защитные механизмы.

Согласно "Оранжевой книге", политика безопасности должна обязательно включать в себя следующие элементы:

- произвольное управление доступом;
- безопасность повторного использования объектов;
- метки безопасности;
- принудительное управление доступом.

Произвольное управление доступом (называемое иногда дискреционным) — это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.

Для реализации принудительного управления доступом с субъектами и объектами ассоциируются метки безопасности. Метка субъекта описывает его благонадежность, метка объекта — степень конфиденциальности содержащейся в нем информации.

Согласно "Оранжевой книге", метки безопасности состоят из двух частей — уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество, категории..— неупорядоченное. Назначение последних — описать предметную область, к которой относятся данные.

Принудительное (или мандатное) управление доступом основано на сопоставлении меток безопасности субъекта и объекта.

Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта.

Описанный способ управления доступом называется принудительным, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы метки безопасности субъектов и объектов, оказываются зафиксированными и права доступа.

Если фиксировать все события, объем регистрационной информации, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. "Оранжевая книга" предусматривает наличие средств выборочного протоколирования, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

Переходя к пассивным аспектам защиты, укажем, что в "Оранжевой книге" рассматривается два вида гарантированности - операционная и технологическая. Операционная гарантированность относится к архитектурным реализационным аспектам системы, в то время как технологическая — к методам построений и сопровождения.

Операционная гарантированность включает в себя проверку следующих элементов:

- архитектура системы;
- целостность системы;
- проверка тайных каналов передачи информации;
- доверенное администрирование;
- доверенное восстановление после сбоев

Технологическая гарантированность охватывает весь жизненный цикл системы, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные "закладки".

Рекомендации X.800

Рекомендации X.800 - документ довольно обширный. Остановимся на специфических сетевых функциях (сервисах) безопасности, а также на необходимых для их реализации защитных механизмах.

Выделяют следующие сервисы безопасности и исполняемые ими роли:

Аутентификация. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

Управление доступом. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

Конфиденциальность данных. Обеспечивает защиту от несанкционированного получения информации. Отдельно упомянем конфиденциальность трафика (это защита информации, которую можно получить, анализируя сетевые потоки данных).

Целостность данных подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры — с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:

- администрирование информационной системы в целом;
- администрирование сервисов безопасности;
- администрирование механизмов безопасности.

Среди действий, относящихся к ИС в целом, отметим обеспечение актуальности политики безопасности, взаимодействие с другими административными службами, реагирование на происходящие события, аудит и безопасное восстановление.

Администрирование сервисов безопасности включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности, комбинирование механизмов для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов. Типичный список таков:

- управление ключами /генерация и распределение);
- управление шифрованием (установка и синхронизация криптографических параметров). К управлению шифрованием можно отнести и администрирование механизмов электронной подписи;
- администрирование управления доступом (распределение информации, необходимой для управления - паролей, списков доступа и т.п.);
- управление аутентификацией (распределение информации, необходимой для аутентификации (паролей, ключей и т.п.);
- управление дополнением трафика (выработка и поддержание правил, задающих характеристик дополняющих сообщений - частоту отправки, размер и т.п.);
- управление маршрутизацией (выделение доверенных путей);
- управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

Сетевые механизмы безопасности

Для реализации сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации:

- шифрование;
- электронная цифровая подпись;
- механизмы управления доступом. Могут располагаться на любой из участвующих в общении сторон или в промежуточной точке;
- механизмы контроля целостности данных. В рекомендациях X.800 различаются два аспекта целостности: целостность от дельного сообщения или поля информации и целостность

потока сообщений или полей информации. Для проверки целостности потока сообщений (то есть для защиты от кражи, переупорядочивания, дублирования и вставки сообщений) используются порядковые номера, временные штампы, криптографическое связывание или иные аналогичные приемы;

- механизмы аутентификации. Согласно рекомендациям X.800, аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик;
- механизмы дополнения трафика;
- механизмы управления маршрутизацией. Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными;
- механизмы нотаризации. Служат для заверения таких, коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией.

Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба.

По историческим причинам данный стандарт часто называют "Общими критериями" (или даже ОК).

"Общие критерии" на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от "Оранжевой книги", ОК не содержат определенных "классов безопасности". Такие классы можно строить, исходя из требований безопасности существующих для конкретной организации и/или конкретной информационной системы.

Как и "Оранжевая книга" ОК содержат два основных вида требований безопасности:

функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;

требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного объекта оценки - аппаратно-программного продукта или информационной системы.

В ОК объект оценки рассматривается в контексте среды безопасности, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка в:

- требованиях безопасности;
- проектировании;
- эксплуатации.

Слабые места по возможности следует устранить, минимизировать или хотя бы постараться ограничить возможный ущерб от их преднамеренного использования или случайной активизации.

В ОК введена иерархия класс-семейство-компонент-элемент.

Классы определяет наиболее общую, "предметную" группировку требований.

Семейства различаются по строгости и другим нюансам требований.

Компонент - минимальный набор требований, фигурирующий как целое.

Элемент — неделимое целое.

Как и между библиотечными функциями, между компонентами ОК могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения цели безопасности.

Профиль защиты (ПЗ) представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в "Общих критериях" представлено 11 функциональных классов, *66* семейств, 135 компонентов.

Перечислим классы функциональных требований ОК:

- идентификация и аутентификация;
- защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
- управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
- аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
- доступ к объекту оценки;
- приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
- использование ресурсов (требования к доступности информации);
- криптографическая поддержка (управление ключами);
- связь (аутентификация сторон, участвующих в обмене данными);
- доверенный маршрут/канал (для связи с сервисами безопасности).

В современном программировании ключевым является вопрос накопления и многократного использования знаний. Стандарты — одна из форм накопления знаний.

Установление доверия безопасности, согласно "Общим критериям", основывается на активном исследовании объекта оценки.

Форма представления требований доверия, в принципе, та же, что и для функциональных требований. Специфика состоит в том, что каждый элемент требований доверия принадлежит одному из трех типов:

- действия разработчиков;
- представление и содержание свидетельств;
- действия оценщиков.

Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности. Перечислим классы:

- разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);
- поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);
- тестирование;
- оценка уязвимостей (включая оценку стойкости функций безопасности);
- поставка и эксплуатация;
- управление конфигурацией;
- руководства (требования к эксплуатационной документации);
- поддержка доверия ;
- оценка профиля защиты;
- оценка задания по безопасности.

Гостехкомиссия России ведет весьма активную нормотворческую деятельность, выпуская Руководящие документы (РД), играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на "Общие критерии", что можно только приветствовать.

Рассмотрим два важных, хотя и не новых, Руководящих документа — Классификацию автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД) и аналогичную Классификацию межсетевых экранов (МЭ).

Согласно первому из них, устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности.

Группа содержит два класса — 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов — 1Д, 1Г, 1В, 1Б и 1А.

Переходя к рассмотрению второго РД Гостехкомиссии России — Классификации межсетевых экранов — укажем, что данный РД представляется принципиально важным, поскольку в нем идет речь не о целостном продукте или системе, а об отдельном сервисе безопасности, обеспечивающем межсетевое разграничение доступа.

Основным критерием классификации МЭ служит протокольный уровень (в соответствии с эталонной семиуровневой моделью), на котором осуществляется фильтрация информации. Это понятно: чем выше уровень, тем больше информации на нем доступно и, следовательно, тем более тонкую и надежную фильтрацию можно реализовать.

Значительное внимание в РД уделено собственной безопасности служб обеспечения защиты и вопросам согласованного администрирования распределенных конфигураций.

Тема 5. Административный уровень информационной безопасности. Управление рисками

К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые руководством организации.

Главная цель мер административного уровня — сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Под политикой безопасности будем понимать совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

Чтобы рассматривать ИС предметно, с использованием актуальных данных, следует составить кварту информационной системы. Эта карта, разумеется, должна быть изготовлена в объектно-ориентированном стиле, с возможностью варьировать не только уровень детализации, но и видимые грани объектов. Техническим средством составления, сопровождения и визуализации подобных карт может служить свободно распространяемый каркас какой-либо системы управления.

Политика безопасности

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Примерный список подобных решений может включать в себя следующие элементы:

- решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;
- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда буферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
- организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их зашиты;
- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки

персонала, порядок реагирования на нарушения режима безопасности и т.п.);

- раздел, освещающий вопросы физической защиты;
- управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
- раздел, описывающий правила разграничения доступа к производственной информации;
- раздел, характеризующий порядок разработки и сопровождения систем;
- раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;
- юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем. Примеры таких вопросов — отношение к передовым (но, возможно, недостаточно проверенным) технологиям, доступ в Internet (как совместить свободу доступа к информации с защитой от внешних угроз?), использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Политика среднего уровня должна для каждого аспекта освещать следующие, темы:

- Описание аспекта.
- Область применения.

- Позиция организации по данному аспекту.
- Роли и обязанности.
- Законопослушность.
- Точки контакта.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она включает в себя два аспекта — цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время, эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?
- как организован удаленный доступ к сервису?

Программа безопасности

После того, как сформулирована политика безопасности, можно приступать к составлению программы ее реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, её нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространенном случае достаточно двух уровней — верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. У этой программы следующие главные цели:

- управление рисками (оценка рисков, выбор эффективных средств защиты);
- координация деятельности в области информационной безопасности, пополнение и распределение ресурсов;
- стратегическое планирование;
- контроль деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, и необходимо иметь четкую политику отслеживания и внедрения новых средств.

Программа верхнего уровня должна занимать строго определенное место в деятельности организации, она должна официально приниматься и поддерживаться руководством, а также иметь определенный штат и бюджет.

Цель программы нижнего уровня — обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупаются и устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест и т.п. Обычно за программу нижнего уровня отвечают администраторы сервисов.

Синхронизация программы безопасности с жизненным циклом систем

В жизненном цикле информационного сервиса можно выделить следующие этапы:

Инициация. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.

Закупка. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.

Установка. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.

Эксплуатация. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

Выведение из эксплуатации. Происходит переход на новый сервис.

Управление рисками

Управление рисками, равно как и выработка собственной политики безопасности, актуально только для тех организаций, информационные системы которых и/или обрабатываемые данные можно считать нестандартными. Обычную организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков. Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество бумаг, во втором достаточно определиться лишь с несколькими параметрами.

Использование информационных систем связано с определенной совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая (пере)оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

С количественной точки зрения уровень риска является функцией вероятности реализации определенной угрозы, а также величины возможного ущерба.

Суть мероприятий по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми). Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

- (пере)оценка (измерение) рисков;
- выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска (например, за счет устранения причины);
- уменьшение риска (например, за счет использования дополнительных защитных средств);
- принятие риска (и выработка плана действия в соответствующих условиях);
- переадресация риска (например, путем заключения страхового соглашения).

Процесс управления рисками можно разделить на следующие этапы:

1. Выбор анализируемых объектов и уровня детализации их рассмотрения.
2. Выбор методологии оценки рисков.
3. Идентификация активов.
4. Анализ угроз и их последствий, выявление уязвимых мест в защите.
5. Оценка рисков.
6. Выбор защитных мер.
7. Реализация и проверка выбранных мер.
8. Оценка остаточного риска.

Подготовительные этапы управления рисками

Выбор анализируемых объектов и уровня детализации их рассмотрения — первый шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру; однако если организация крупная, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближенностью итоговой оценки. Если важных сервисов все еще много, выбираются те из них, риски для которых заведомо велики или неизвестны.

Очень важно выбрать разумную методологию оценки рисков. Целью оценки является получение ответа на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства стоит использовать. Значит, оценка должна быть количественной, допускающей сопоставление с заранее выбранными границами допустимости и расходами на реализацию новых регуляторов безопасности. Управление рисками — типичная оптимизационная задача, и существует довольно много программных продуктов, способных помочь в ее решении . Принципиальная трудность, однако, состоит в неточности исходных данных. Практичнее пользоваться условными единицами. В простейшем и вполне допустимом случае можно пользоваться трехбалльной шкалой.

При идентификации активов, то есть тех ресурсов и ценностей, которые организация пытается защитить, следует, конечно, учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как репутация организации.

Информационной основой сколько-нибудь крупной организации является сеть, поэтому в число аппаратных активов следует включить компьютеры (серверы, рабочие станции, ПК), периферийные устройства, внешние интерфейсы, кабельное хозяйство, активное сетевое оборудование. К программным активам, вероятно, будут отнесены операционные системы, прикладное программное обеспечение, инструментальные средства, средства управления сетью и отдельными системами. Третьим видом информационных активов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, способы доступа к ним. Все это важно для оценки последствий нарушений информационной безопасности.

Основные этапы управления рисками

Этапы, предшествующие анализу угроз, можно считать подготовительными, поскольку, строго говоря, они напрямую с рисками не связаны. Риск появляется там, где есть угрозы.

Первый шаг в анализе угроз – их идентификация. Рассматриваемые виды угроз следует выбирать исходя из соображений здравого смысла (исключив, например, землетрясения, однако не забывая о возможности захвата организации террористами), но в пределах выбранных видов провести максимально подробный анализ.

После идентификации угрозы необходимо оценить вероятность ее осуществления. Допустимо использовать при этом трехбалльную шкалу (низкая (1), средняя (2) и высокая (3) вероятность).

Кроме вероятности осуществления, важен размер потенциального ущерба. Например, пожары бывают нечасто, но ущерб от каждого из них, как правило, велик. Тяжесть ущерба также можно оценить по трехбалльной шкале.

После того, как накоплены исходные данные и оценена степень неопределенности, можно переходить к обработке информации, то есть собственно к оценке рисков. Вполне допустимо применить такой простой метод, как умножение вероятности осуществления угрозы на предполагаемый ущерб. Если для вероятности и ущерба использовать трехбалльную шкалу, то возможных произведений будет шесть: 1, 2, 3, 4, 6 и 9. Первые два результата можно отнести к низкому риску, третий и четвертый — к среднему, два последних — к высокому, после чего появляется возможность снова привести их к трехбалльной шкале. По этой шкале и следует оценивать приемлемость рисков.

Если какие-либо риски оказались недопустимо высокими, необходимо их нейтрализовать, реализовав дополнительные меры защиты. Как правило, для ликвидации или нейтрализации уязвимого места, сделавшего угрозу реальной, существует несколько механизмов безопасности, различных по эффективности и стоимости.

Оценивая стоимость мер защиты, приходится, разумеется, учитывать не только прямые расходы на закупку оборудования и/или программ, но и расходы на внедрение новинки и, в частности, обучение и переподготовку персонала. Эту стоимость также можно оценить по трехбалльной шкале и затем сопоставить ее с разностью между вычисленным и допустимым риском.

Когда намеченные меры приняты, необходимо проверить их действенность, то есть убедиться, что остаточные риски стали приемлемыми. Если это на самом деле так, значит, можно спокойно намечать дату ближайшей переоценки. В противном случае придется проанализировать допущенные ошибки и провести повторный сеанс управления рисками немедленно.

Тема 6. Процедурный уровень информационной безопасности

На процедурном уровне можно выделить следующие классы мер:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Управление персоналом

Управление персоналом начинается с приема нового сотрудника на работу и даже раньше — с составления описания должности. Уже на данном этапе желательно подключить к работе специалиста по информационной безопасности для определения компьютерных привилегий, ассоциируемых с должностью. Существует два общих принципа, которые следует иметь в виду:

- разделение обязанностей;
- минимизация привилегий.

Предварительное составление описания должности позволяет оценить ее критичность и спланировать процедуру проверки и отбора кандидатов.

Когда кандидат определен, он, должен пройти обучение, его следует подробно ознакомить со служебными обязанностями, а также с нормами и процедурами информационной безопасности. Желательно, чтобы меры безопасности были им усвоены до вступления в должность и до заведения его системного счета с входным именем, паролем и привилегиями.

С момента заведения системного счета начинается его администрирование, а также протоколирование и анализ действий пользователя. Постепенно изменяется окружение, в котором работает пользователь, его служебные обязанности и т.п. Все это требует соответствующего изменения привилегий. Техническую сложность представляют временные перемещения пользователя, выполнение им обязанностей взамен сотрудника, ушедшего в отпуск, и иные обстоятельства, когда полномочия нужно сначала предоставить, а через некоторое время взять обратно. В такие периоды профиль активности пользователя резко меняется, что создает трудности при выявлении подозрительных ситуаций. Определенную аккуратность следует соблюдать и при выдаче новых постоянных полномочий, не забывая ликвидировать старые права доступа.

Ликвидация системного счета пользователя, особенно в случае конфликта между сотрудником и организацией, должна производиться максимально оперативно. Возможно и физическое ограничение доступа к рабочему месту. Разумеется, если сотрудник увольняется, у него нужно принять все его компьютерное хозяйство и, в частности, криптографические ключи, если использовались средства шифрования.

Физическая защита

Безопасность информационной системы зависит от окружения, в котором она функционирует. Необходимо принять меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры, вычислительной техники, носителей данных.

Рассмотрим следующие направления физической защиты:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры;
- защита от перехвата данных;
- защита мобильных систем.

Меры физического управления доступом позволяют контролировать и при необходимости ограничивать вход и выход сотрудников и посетителей. Контролироваться может все здание организации, а также отдельные помещения, например, те, где расположены серверы, коммуникационная аппаратура и т.п.

Средства физического управления доступом известны давно. Это охрана, двери с замками, перегородки, телекамеры, датчики движения и многое другое. Для выбора оптимального (по критерию стоимость/эффективность) средства целесообразно провести анализ рисков. Кроме того, есть смысл периодически отслеживать появление технических новинок в данной области, стараясь максимально автоматизировать физическую защиту.

Профессия пожарника — одна из древнейших, но пожары по-прежнему случаются и наносят большой ущерб. Необходимость установки противопожарной сигнализации и автоматических средств пожаротушения очевидна.

К поддерживающей инфраструктуре можно отнести системы электро-, водо- и теплоснабжения, кондиционеры и средства коммуникаций. В принципе, к ним применимы те же требования целостности и доступности, что и к информационным системам. Для обеспечения целостности нужно защищать оборудование от краж и повреждений. Для поддержания доступности следует выбирать оборудование с максимальным временем наработки на отказ, дублировать ответственные узлы и всегда иметь под рукой запчасти.

Мобильные и портативные компьютеры — заманчивый объект кражи. Их часто оставляют без присмотра, в автомобиле или на работе, и похитить такой компьютер совсем несложно. То и дело средства массовой информации сообщают о том, что какой-нибудь офицер английской разведки или американский военный лишился таким образом движимого имущества. Мы настоятельно рекомендуем шифровать данные на жестких дисках таких компьютеров.

Поддержание работоспособности

Нечаянные ошибки системных администраторов и пользователей грозят повреждением аппаратуры, разрушением программ и данных; в лучшем случае они создают бреши в защите, которые делают возможной реализацию угроз.

Выделим следующие направления повседневной деятельности:

- поддержка пользователей;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;

Поддержка пользователей подразумевает прежде всего консультирование и оказание помощи при решении разного рода проблем. Целесообразно фиксировать вопросы пользователей, чтобы выявлять их типичные ошибки и выпускать памятки с рекомендациями для распространенных ситуаций.

Поддержка программного обеспечения - одно из важнейших средств обеспечения целостности информации. Прежде всего, необходимо следить за тем, какое программное обеспечение установлено на компьютерах.

Второй аспект поддержки программного обеспечения — контроль за отсутствием неавторизованного изменения программ и прав доступа к ним. Обычно контроль достигается комбинированием средств физического и логического управления доступом, а также использованием утилит проверки и обеспечения целостности.

Лучший способ уменьшить количество ошибок в рутинной работе — максимально автоматизировать ее. Правы те ленивые программисты и системные администраторы, которые, окинув взглядом море однообразных задач, говорят: "Я ни за что не буду делать этого, я напишу программу, которая сделает все за меня". Автоматизация и безопасность зависят друг от друга; тот, кто заботится в первую очередь об облегчении своей задачи, на самом деле оптимальным образом формирует режим информационной безопасности.

Резервное копирование необходимо для восстановления программ и данных после аварий. Нужно также наладить размещение копий в безопасном месте, защищенном от несанкционированного доступа, пожаров, протечек, то есть от всего, что может привести к краже или повреждению носителей.

Управлять носителями необходимо для обеспечения физической защиты и учета дискет, лент, печатных выдач и т.п. Управление носителями должно обеспечивать конфиденциальность, целостность и доступность информации, хранящейся вне компьютерных систем. Под физической защитой здесь понимается не только отражение попыток несанкционированного доступа, но и предохранение от вредных влияний окружающей среды (жары, холода, влаги, магнетизма).

Документирование — неотъемлемая часть информационной безопасности. В виде документов оформляется почти все — от политики безопасности до журнала учета носителей. Важно, чтобы документация была актуальной, отражала именно текущее состояние дел, причем в непротиворечивом виде.

Реагирование на нарушения режима безопасности

Программа безопасности, принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности.

Реакция на нарушения режима безопасности преследует три главные цели:

- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных нарушений.

В организации должен быть человек доступный 24 часа в сутки (лично, по телефону, пейджеру или электронной почте), который отвечает за реакцию на нарушения. Все должны знать координаты этого человека и обращаться к нему при первых признаках опасности.

Нередко требование локализации инцидента и уменьшения наносимого вреда вступает в конфликт с желанием выявить нарушителя. В политике безопасности организации приоритеты должны

быть расставлены заранее. Поскольку, как показывает практика, выявить злоумышленника очень сложно, на наш взгляд, в первую очередь следует заботиться об уменьшении ущерба.

Чтобы предотвратить повторные нарушения, необходимо анализировать каждый инцидент, выявлять причины, накапливать статистику.

Необходимо отслеживать появление новых уязвимых мест и как можно быстрее ликвидировать ассоциированные с ними окна опасности. Кто-то в организации должен курировать этот процесс, принимать краткосрочные меры и корректировать программу безопасности для принятия долгосрочных мер.

Планирование восстановительных работ

Планирование восстановительных работ позволяет подготовиться к авариям, уменьшить ущерб от них, сохранить способность к функционированию хотя бы в минимальном объеме.

Процесс планирования восстановительных работ можно разделить на следующие этапы:

- выявление критически важных функций организации, установление приоритетов;
- идентификация ресурсов, необходимых для выполнения критически важных функций;
- определение перечня возможных аварий;
- разработка стратегии восстановительных работ;
- подготовка к реализации выбранной стратегии;
- проверка стратегии.

Планируя восстановительные работы, следует отдавать себе отчет в том, что полностью сохранить функционирование организации не всегда возможное. Необходимо выявить критически важные функции, без которых организация теряет свое лицо, и даже среди критичных функций расставить приоритеты, чтобы как можно быстрее и с минимальными затратами возобновить работу после аварии.

Критичные ресурсы обычно относятся к одной из следующих категорий:

- персонал;
- информационная инфраструктура;
- физическая инфраструктура.

Составляя списки ответственных специалистов, следует учитывать, что некоторые из них могут непосредственно пострадать от аварии (например, от пожара), кто-то может находиться в состоянии стресса, часть сотрудников, возможно, будет лишена возможности попасть на работу (например, в случае массовых беспорядков).

Информационная инфраструктура включает в себя следующие элементы:

- компьютеры;
- программы и данные;
- информационные сервисы внешних организаций;
- документацию.

К физической инфраструктуре относятся здания, инженерные коммуникации, средства связи, оргтехника и многое другое. Компьютерная техника не может работать в плохих условиях, без стабильного электропитания и т.п.

Стратегия восстановительных работ должна базироваться на наличных ресурсах и быть не слишком накладной для организации. При разработке стратегии целесообразно провести анализ рисков, которым подвергаются критичные функции, и попытаться выбрать наиболее экономичное решение. Стратегия должна предусматривать не только работу по временной схеме, но и возвращение к нормальному функционированию.

Подготовка к реализации выбранной стратегии состоит в выработке плана действий в экстренных ситуациях и по их окончании, а также в обеспечении некоторой избыточностей критичных ресурсов.

Проверка стратегии производится путем анализа подготовленного плана, принятых и намеченных мер.

Тема 7. Основные программно-технические меры

Программно-технические меры, то есть меры, направленные на контроль компьютерных сущностей — оборудования, программ и/или данных, образует последний и самый важный рубеж информационной безопасности. Компьютеры помогли автоматизировать многие области человеческой

деятельности. Вполне естественным представляется желание возложить на них и обеспечение собственной безопасности. Даже физическую защиту все чаще поручают не охранникам, а интегрированным компьютерным системам, что позволяет одновременно отслеживать перемещения сотрудников и по организации, и по информационному пространству.

Следует, однако, учитывать, что быстрое развитие информационных технологий не только предоставляет обороняющимся новые возможности, но и объективно затрудняет обеспечение надежной защиты, если опираться исключительно на меры программно-технического уровня. Причин тому несколько:

- повышение быстродействия микросхем, развитие архитектур с высокой степенью параллелизма позволяет методом грубой силы преодолевать барьеры (прежде всего криптографические), ранее казавшиеся неприступными;
- развитие сетей и сетевых технологий, увеличение числа связей между информационными системами, рост пропускной способности каналов расширяют круг злоумышленников, имеющих техническую возможность организовывать атаки;
- появление новых информационных сервисов ведет и к образованию новых уязвимых мест как "внутри" сервисов, так и на их стыках;
- конкуренция среди производителей программного обеспечения заставляет сокращать сроки разработки, что приводит к снижению качества тестирования и выпуску продуктов с дефектами защиты;
- навязываемая потребителям парадигма постоянного наращивания мощности аппаратного и программного обеспечения не позволяет долго оставаться в рамках надежных, апробированных конфигураций и, кроме того, вступает в конфликт с бюджетными ограничениями, из-за чего снижается доля ассигнований на безопасность.

Центральным для программно-технического уровня является понятие сервиса безопасности.

Рассмотрим следующие сервисы:

1. идентификация и аутентификация;
2. управление доступом;
3. протоколирование и аудит;
4. шифрование;
5. контроль целостности;
6. экранирование;
7. анализ защищенности;
8. обеспечение отказоустойчивости;
9. обеспечение безопасного восстановления;
10. туннелирование;
11. управление.

Совокупность перечисленных сервисов безопасности будем называть полным набором.

Для проведения классификации сервисов безопасности и определения их места в общей архитектуре меры безопасности можно разделить на следующие виды:

- превентивные, препятствующие нарушениям ИБ;
- меры обнаружения нарушений;
- локализующие, сужающие зону воздействия нарушений;
- меры по выявлению нарушителя;
- меры восстановления режима безопасности.

Информационная система "типичной современной организации является весьма сложным образованием, построенным в многоуровневой архитектуре клиент/сервер, которое пользуется многочисленными внешними сервисами и, в свою очередь, предоставляет собственные сервисы вовне. Даже сравнительно небольшие магазины, обеспечивающие расчет с покупателями по пластиковым картам, зависят от своих информационных систем и, в частности, от защищенности всех компонентов систем и коммуникаций между ними.

С точки зрения безопасности наиболее существенными представляются следующие аспекты современных ИС:

- корпоративная сеть имеет несколько территориально разнесенных частей (поскольку орга-

низация располагается на нескольких производственных площадках), связи между которыми находятся в ведении внешнего поставщика сетевых услуг, выходя за пределы зоны, контролируемой организацией;

- корпоративная сеть имеет одно или несколько подключений к Internet;
- на каждой из производственных площадок могут находиться критически важные серверы, в доступе к которым нуждаются сотрудники, работающие на других площадках, мобильные пользователи и, возможно, сотрудники других организаций;
- для доступа пользователей могут применяться не только компьютеры, но и потребительские устройства, использующие, в частности, беспроводную связь;
- в течение одного сеанса работы пользователю приходится обращаться к нескольким информационным сервисам, опирающимся на разные аппаратно-программные платформы;
- к доступности информационных сервисов предъявляются жесткие требования, которые обычно выражаются в необходимости круглосуточного функционирования с максимальным временем простоя порядка нескольких минут;
- информационная система представляет собой сеть с активными агентами, то есть в процессе работы программные компоненты, такие как апплеты или сервлеты, передаются с одной машины на другую, и выполняются в целевой среде, поддерживая связь с удаленными компонентами;
- не все пользовательские системы контролируются сетевыми и/или системными администраторами организации; программное обеспечение, особенно полученное по сети, не может считаться надежным, в нем могут быть ошибки, создающие проблемы в защите;
- конфигурация информационной системы постоянно изменяется на уровнях административных данных, программ и аппаратуры (меняется состав пользователей, их привилегии и версии программ, появляются новые сервисы, новая аппаратура и т.п.).

Архитектурная безопасность

Сервисы безопасности, какими бы мощными они ни были, сами по себе не могут гарантировать надежность программно-технического уровня защиты. Только проверенная архитектура способна сделать эффективным объединение сервисов, обеспечить управляемость информационной системы, ее способность развиваться и противостоять новым угрозам при сохранении таких свойств, как высокая производительность, простота и удобство использования.

Если какой-либо (составной) сервис не обладает полным набором защитных средств (состав полного набора описан выше), необходимо привлечение дополнительных сервисов, которые будем называть экранирующими. Экранирующие сервисы устанавливаются на путях доступа к недостаточно защищенным элементам; в принципе, один такой сервис может экранировать (защищать) сколь угодно большое число элементов.

С практической точки зрения наиболее важными являются следующие принципы архитектурной безопасности:

- непрерывность защиты в пространстве и времени, невозможность миновать защитные средства;
- следование признанным стандартам, использование апробированных решений;
- иерархическая организация ИС с небольшим числом сущностей на каждом уровне;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;
- разделение обязанностей;
- эшелонированность обороны;
- разнообразие защитных средств;
- простота и управляемость информационной системы.

Для обеспечения высокой доступности (непрерывности функционирования) необходимо соблюдать следующие принципы архитектурной безопасности:

- внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.);
- наличие средств обнаружения нештатных ситуаций;

- наличие средств реконфигурирования для восстановления, изоляции и/или замены компонентов, отказавших или подвергшихся атаке на доступность;
- выделение подсетей и изоляция групп пользователей друг от друга. Данная мера, являющаяся обобщением разделения процессов на уровне операционной системы, ограничивает зону поражения при возможных нарушениях информационной безопасности.

Еще один важный архитектурный принцип — минимизация объема защитных средств, выносимых на клиентские системы. Причин тому несколько:

- для доступа в корпоративную сеть могут использоваться потребительские устройства с ограниченной функциональностью;
- конфигурацию клиентских систем трудно или невозможно контролировать.

Тема 8. Идентификация и аутентификация, управление доступом

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Идентификация и аутентификация – это первая линия обороны, "проходная" информационного пространства организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

В сетевой среде, когда стороны идентификации/аутентификации территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

- что служит аутентификатором (то есть используется для подтверждения подлинности субъекта);
- как организован (и защищен) обмен данными идентификации/аутентификации.

Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:

- нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);
- нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).

В открытой сетевой среде между сторонами идентификации/аутентификации не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от перехвата, изменения и/или воспроизведения данных. Передача паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от воспроизведения. Нужны более сложные протоколы аутентификации.

Сервис идентификации/аутентификации может стать объектом атак на доступность. Если система сконфигурирована так, что после определенного числа неудачных попыток устройство ввода идентификационной информации (такое, например, как терминал) блокируется, то злоумышленник может остановить работу легального пользователя буквально несколькими нажатиями клавиш.

Парольная аутентификация

Главное достоинство парольной аутентификации — простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т.п.). Однако простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя.

Иногда пароли с самого начала не хранятся в тайне, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена.

Пароли нередко сообщают коллегам, чтобы те могли, например, подменить на некоторое время владельца пароля. Теоретически в подобных случаях более правильно задействовать средства управления доступом, но на практике так никто не поступает; а тайна, которую знают двое, это уже не тайна.

Пароль можно угадать "методом грубой силы", используя, скажем, словарь. Если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор (предполагается, что алгоритм шифрования известен).

Одноразовые пароли

Рассмотренные выше пароли можно назвать многоразовыми; их раскрытие позволяет злоумышленнику действовать от имени легального пользователя. Гораздо более сильным средством, устойчивым к пассивному прослушиванию сети, являются одноразовые пароли.

Наиболее известным программным генератором одноразовых паролей является система S/KEY компании Bellcore. Идея этой системы состоит в следующем. Пусть имеется односторонняя функция f (то есть функция, вычислить обратную которой за приемлемое время не представляется возможным). Эта функция известна и пользователю, и серверу аутентификации. Пусть, далее, имеется секретный ключ К, известный только пользователю.

На этапе начального администрирования пользователя функция f применяется к ключу К n раз, после чего результат сохраняется на сервере. После этого процедура проверки подлинности пользователя выглядит следующим образом:

- сервер присылает на пользовательскую систему число (n -1);
- пользователь применяет функцию f к секретному ключу К (n-1) раз и отправляет результат по сети на сервер аутентификации;
- сервер применяет функцию f к полученному от пользователя значению и сравнивает результат с ранее сохраненной величиной. В случае совпадения подлинность пользователя считается установленной, сервер запоминает новое значение (присланное пользователем) и уменьшает на единицу счетчик (n).

На самом деле реализация устроена чуть сложнее (кроме счетчика, сервер посылает затравочное значение, используемое функцией f), но для нас сейчас это не важно. Поскольку функция f необратима, перехват пароля, равно как и получение доступа к серверу аутентификации, не позволяют узнать секретный ключ К и предсказать следующий одноразовый пароль.

Система S/KEY имеет статус Internet-стандарта (RFC 1938)

Другой подход к надежной аутентификации состоит в генерации нового пароля через небольшой промежуток времени (например, каждые 60 секунд), для чего могут использоваться, программы или специальные интеллектуальные карты (с практической точки зрения такие пароли можно считать одноразовыми). Серверу аутентификации должен быть известен алгоритм генерации паролей и ассоциированные с ним параметры; кроме того, часы клиента и сервера должны быть синхронными.

Идентификация/аутентификация с помощью биометрических данных

Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

Биометрией во всем мире занимаются очень давно, однако долгое время все, что было связано с ней, отличалось сложностью и дороговизной. В последнее время спрос на биометрические продукты, в первую очередь в связи с развитием электронной коммерции, постоянно и весьма интенсивно растет. Это понятно, поскольку с точки зрения пользователя гораздо удобнее предъявить себя самого, чем что-то запоминать. Спрос рождает предложение, и на рынке появились относительно недорогие аппаратно-программные продукты, ориентированные в основном на распознавание отпечатков пальцев.

Обычно биометрию применяют вместе с другими аутентификаторами, такими, например, как интеллектуальные карты. Иногда биометрическая аутентификация является лишь первым

рубежом защиты и служит для активизации интеллектуальных карт, хранящих криптографические секреты; в таком с случае биометрический шаблон хранится на той же карте.

Управление доступом

С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами). Логическое управление доступом — это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций (зависящее, быть может, от некоторых дополнительных условий) и контролировать выполнение установленного порядка.

Отношение "субъекты-объекты" можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах — объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа.

Тема логического управления доступом — одна из сложнейших в области информационной безопасности. Дело в том, что само понятие объекта (а тем более видов доступа) меняется от сервиса к сервису. Для операционной системы к объектам относятся файлы, устройства и процессы. Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа другим субъектам (так называемое право владения). Процессы можно создавать и уничтожать. Современные операционные системы могут поддерживать и другие объекты.

Для систем управления реляционными базами данных объект — это база данных, таблица, представление, хранимая процедура. К таблицам применимы операции поиска, добавления, модификации и удаления данных, у других объектов иные виды доступа.

Разнообразие объектов и применимых к ним операций приводит к принципиальной децентрализации логического управления доступом. Каждый сервис должен сам решать, позволить ли конкретному субъекту ту или иную операцию. Теоретически это согласуется с современным объектно-ориентированным подходом, на практике же приводит к значительным трудностям. Главная проблема в том, что ко многим объектам можно получить доступ с помощью разных сервисов (возможно, при этом придется преодолеть некоторые технические трудности). Так, до реляционных таблиц можно добраться не только средствами СУБД, но и путем непосредственного чтения файлов или дисковых разделов, поддерживаемых операционной системой (разобравшись предварительно в структуре хранения объектов базы данных). В результате при задании матрицы доступа нужно принимать во внимание не только принцип распределения привилегий для каждого сервиса, но и существующие связи между сервисами (приходится заботиться о согласованности разных частей матрицы). Аналогичная трудность возникает при экспорте/импорте данных, когда информация о правах доступа, как правило, теряется (поскольку на новом сервисе она не имеет смысла). Следовательно, обмен данными между различными сервисами представляет особую опасность с точки зрения управления доступом, а при проектировании и реализации разнородной конфигурации необходимо позаботиться о согласованном распределении прав доступа субъектов к объектам и о минимизации числа способов экспорта/импорта данных.

Матрицу доступа, ввиду ее разреженности (большинство клеток — пустые), неразумно хранить в виде двухмерного массива. Обычно ее хранят по столбцам, то есть для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами. Элементами списков могут быть имена групп и шаблоны субъектов, что служит большим подспорьем администратору. Некоторые проблемы возникают только при удалении субъекта, когда приходится удалять его имя из всех списков доступа; впрочем, эта операция производится нечасто.

Списки доступа — исключительно гибкое средство. Посредством списков несложно добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы

пользователей). Безусловно, списки являются лучшим средством произвольного управления доступом.

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Подобный подход обычно реализуют в рамках системы меню (пользователю показывают лишь допустимые варианты выбора) или посредством ограничивающих оболочек.

Ролевое управление доступом

При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимы решения в объектно-ориентированном стиле, способные эту сложность понизить.

Таким решением является ролевое управление доступом (РУД). Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности — роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права.

Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах.

Ролевой доступ развивается более 10 лет (сама идея ролей, разумеется, значительно старше) как на уровне операционных систем, так и в рамках СУБД и других информационных сервисов. В частности, существуют реализации ролевого доступа для Web-серверов.

В 2001 году Национальный институт стандартов и технологий США предложил проект стандарта ролевого управления доступом.

Ролевое управление доступом оперирует следующими основными понятиями:

- пользователь (человек, интеллектуальный автономный агент и т.п.);
- сеанс работы пользователя;
- роль (обычно определяется в соответствии с организационной структурой);
- объект (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД);
- операция (зависит от объекта; для файлов ОС — чтение, запись, выполнение и т.п.; для таблиц СУБД — вставка, удаление и т.п., для прикладных объектов операции могут быть более сложными);
- право доступа (разрешение, выполнять определенные операции над определенными объектами).

Ролям приписываются пользователи и права доступа; можно считать, что они (роли) именуют отношения "многие ко многим" между пользователями и правами. Роли могут быть приписаны многие пользователи; один пользователь может быть приписан нескольким ролям. Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан, в результате чего он становится обладателем объединения прав, приписанных активным ролям. Одновременно пользователь может открыть несколько сеансов.

Отношение наследования является иерархическим, причем права доступа и пользователи распространяются по уровням иерархии навстречу друг другу. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц.

Статическое разделение обязанностей налагает ограничения на приписывание пользователей ролям. В простейшем случае членство в некоторой роли запрещает приписывание пользователя определенному множеству других ролей. В общем случае данное ограничение задается как пара "множество ролей — число" (где множество состоит, по крайней мере, из двух ролей, а число должно быть больше 1), так что никакой пользователь не может быть приписан указанному (или большему) числу ролей из заданного множества. Например, может существовать пять бухгалтерских ролей, но политика безопасности допускает членство не более чем в двух таких ролях (здесь число=3).

При наличии наследования ролей ограничение приобретает несколько более сложный вид, но суть остается простой: при проверке членства в ролях нужно учитывать приписывание пользователей ролям-наследницам.

Тема 9. Протоколирование и аудит, шифрование, контроль целостности

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе. Аудит — это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация протоколирования и аудита решает следующие задачи:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Протоколирование требует для своей реализации здравого смысла. Какие события регистрировать? С какой степенью детализации? На подобные вопросы невозможно дать универсальные ответы. Необходимо следить за тем, чтобы, с одной стороны, достигались перечислен цели, а, с другой, расход ресурсов оставался в пределах допустимого. Слишком обширное или подробное протоколирование не только снижает производительность сервисов (что отрицательно сказывается на доступности), но и затрудняет аудит, то есть не увеличивает, а уменьшает информационную безопасность.

Разумный подход применительно к операционным системам предлагается в "Оранжевой книге", где выделены следующие события:

- вход в систему (успешный или нет);
- выход из системы;
- обращение к удаленной системе;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т.п.).

При протоколировании события рекомендуется записывать, по крайней мере, следующую информацию:

- дата и время события;
- уникальный идентификатор пользователя — инициатора действия;
- тип события;
- результат действия (успех или неудача);
- источник запроса (например, имя терминала);
- имена затронутых объектов (например, открываемых или удаляемых файлов);
- описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта).

Реконструкция последовательности событий позволяет выявить слабости в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе.

Активный аудит

Под подозрительной активностью понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или не типичным (согласно принятым критериям).

Задача активного аудита — оперативно выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нее.

Активность, не соответствующую политике безопасности, целесообразно разделить на атаки, направленные на незаконное получение полномочий, и на действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности.

Атаки нарушают любую осмысленную политику безопасности. Иными словами, активность атакующего является разрушительной независимо от политики. Следовательно, для описания и выявления атак можно применять универсальные методы, инвариантные относительно политики

безопасности, такие как сигнатуры и их обнаружение во входном потоке событий с помощью аппарата экспертных систем.

Сигнатура атаки — это совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию. Простейший пример сигнатуры — "зафиксированы три последовательные неудачные попытки входа в систему с одного терминала", пример ассоциированной реакции — блокирование терминала до прояснения ситуации.

Применительно к средствам активного аудита различают ошибки первого и второго рода: пропуск атак и ложные тревоги, соответственно. Нежелательность ошибок первого рода очевидна; ошибки второго рода не менее неприятны, поскольку отвлекают администратора безопасности от действительно важных дел, косвенно способствуя пропуску атак.

Средства активного аудита могут располагаться на всех линиях обороны информационной системы. На границе контролируемой зоны они могут обнаруживать подозрительную активность в точках подключении к внешним сетям (не только попытки нелегального проникновения, но и действия по "прощупыванию" сервисов безопасности). Важно отметить, что активный аудит, в принципе, способен обеспечить защиту от атак на доступность.

Функциональные компоненты и архитектура

В составе средств активного аудита можно выделить следующие функциональные компоненты:

- компоненты генерации регистрационной информации. Они находятся на стыке между средствами активного аудита и контролируемыми объектами;
- компоненты хранения сгенерированной регистрационной информации;
- компоненты просмотра регистрационной информации. Могут помочь при принятии решения о реагировании на подозрительную активность;
- компоненты анализа информации, поступившей от сенсоров. В соответствии с данным выше определением средств активного аудита, выделяют пороговый анализатор, анализатор нарушений политики безопасности, экспертную систему, выявляющую сигнатуры атак, а также статистический анализатор, обнаруживающий нетипичное поведение;
- компоненты хранения информации, участвующей в анализе. Такое хранение необходимо, например, для выявления атак, протяженных во времени;
- компоненты принятия решений и реагирования ("решатели"). "Решатель" может получать информацию не только от локальных, но и от внешних анализаторов, проводя так называемый корреляционный анализ распределенных событий;
- компоненты хранения информации о контролируемых объектах. Здесь могут храниться как пассивные данные, так и методы, необходимые, например, для извлечения из объекта регистрационной информации или для реагирования;
- компоненты, играющие роль организующей оболочки для менеджеров активного аудита, называемые мониторами и объединяющие анализаторы, "решатели", хранилище описаний объектов и интерфейсные компоненты. В число последних входят компоненты интерфейса с другими мониторами, как равноправными, так и входящими в иерархию. Такие интерфейсы необходимы, например, для выявления распределенных, широкомасштабных атак;
- компоненты интерфейса с администратором безопасности.

Шифрование

Криптография необходима для реализации, по крайней мере, трех сервисов безопасности:

- шифрование;
- контроль целостности;
- аутентификация.

Шифрование — наиболее мощное средство обеспечения конфиденциальности. Во многих отношениях оно занимает центральное место среди програмнно-технических регуляторов, и в то же время последним (а подчас и единственным) защитным рубежом.

В большинстве случаев и шифрование, и контроль целостности играют глубоко инфраструктурную роль, оставаясь прозрачными и для приложений, и для пользователей. Типичное место этих сервисов безопасности – на сетевом и транспортном уровнях реализации стека сетевых протоколов.

Различают два основных метода шифрования: симметричный и асимметричный. В первом из них один и тот же ключ (хранящийся в секрете) используется и для зашифровывания, и для расшифрования данных.

Разработаны весьма эффективные (быстрые и надежные) методы симметричного шифрования. Существует и национальный стандарт на подобные методы – ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".

Для определенности мы будем вести речь о защите сообщений, хотя события могут развиваться не только в пространстве, но и во времени, когда зашифровываются и расшифровываются никуда не перемещающиеся файлы.

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, это создает новую проблему распространения ключей. С другой стороны, получатель на основании наличия зашифрованного и расшифрованного сообщения не может доказать, что он получил это сообщение от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать самостоятельно.

В асимметричных методах используются два ключа. Один из них, несекретный (он может публиковаться вместе с другими открытыми сведениями о пользователе), применяется для шифрования, другой (секретный, известный только получателю) — для расшифрования. Самым популярным из асимметричных является метод RSA (Райвест, Шамир, Адлеман), основанный на операциях с большими (скажем, 100-значными) простыми числами и их произведениями.

Определенное распространение получила разновидность симметричного шифрования, основанная на использовании составных ключей. Идея состоит в том, что секретный ключ делится на две части, хранящиеся отдельно. Каждая часть сама по себе не позволяет выполнить расшифрование. Если у правоохранительных органов появляются подозрения относительно лица, использующего некоторый ключ, они могут в установленном порядке получить половинки ключа и дальше действовать обычным для симметричного расшифрования образом.

Многие криптографические алгоритмы в качестве одного из параметров требуют псевдослучайное значение, в случае предсказуемости которого в алгоритме появляется уязвимость (подобное уязвимое место было обнаружено в некоторых вариантах Web-навигаторов).

Контроль целостности

Криптографические методы позволяют надежно контролировать целостность как отдельных порций данных, так и их наборов (таких как поток сообщений); определять подлинность источника данных; гарантировать невозможность отказаться от совершенных действий («неотказуемость»).

В основе криптографического контроля целостности лежат два понятия:

- хэш-функция;
- электронная цифровая подпись (ЭЦП).

Хэш-функция — это труднообратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции.

Пусть имеются данные, целостность которых нужно проверить, хэш-функция и ранее вычисленный результат ее применения к исходным данным (так называемый дайджест).

Два российских стандарта, ГОСТ Р 34.10-94 "Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма" и ГОСТ Р 34.11-94 "Функция хэширования", объединенные общим заголовком "Информационная технология. Криптографическая защита информации", регламентируют вычисление дайджеста и реализацию ЭЦП. В сентябре 2001 года был утвержден, а 1 июля 2002 года вступил в силу новый стандарт ЭЦП — ГОСТ Р 34.10-2001, разработанный специалистами ФАПСИ.

Цифровые сертификаты

При использовании асимметричных методов шифрования (и, в частности элёктронной цифровой подписи) необходимо иметь гарантию подлинности пары (имя пользователя, открытый ключ пользователя). Для решения этой задачи в спецификациях X.509 вводятся понятия цифрового сертификата и удостоверяющего центра.

Удостоверяющий центр — это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Открытые ключи и другая информация

о пользователях хранится удостоверяющими центрами в виде цифровых сертификатов, имеющих следующую структуру:

- порядковый номер сертификата;
- идентификатор алгоритма электронной подписи;
- имя удостоверяющего центра;
- срок годности;
- имя владельца сертификата (имя пользователя, которому при надлежит сертификат);
- открытые ключи владельца сертификата (ключей может быть несколько);
- идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата;
- электронная подпись, сгенерированная с использованием секретного ключа удостоверяющего центра (подписывается результат хэширования всей информации, хранящейся в сертификате).

Цифровые сертификаты обладают следующими свойствами:

- любой пользователь, знающий открытый ключ удостоверяющего центра, может узнать открытые ключи других клиентов центра и проверить целостность сертификата;
- никто, кроме удостоверяющего центра, не может модифицировать информацию о пользователе без нарушения целостности сертификата.

В спецификациях X.509 не описывается конкретная процедура генерации криптографических ключей и управления ими, однако даются некоторые общие рекомендации. В частности, оговаривается, что пары ключей могут порождаться любым из следующих способов.

- ключи может генерировать сам пользователь. В таком случае секретный ключ не попадает в руки третьих лиц, однако нужно решать задачу безопасной связи с удостоверяющим центром;
- ключи генерирует доверенное лицо. В таком случае приходится решать задачи безопасной доставки секретного ключа владельцу и предоставления доверенных данных для создания сертификата;
- ключи генерируются удостоверяющим центром. В таком случае остается только задача безопасной передачи ключей владельцу.

Цифровые сертификаты в формате X.509 версии 3 стали не только формальным, но и фактическим стандартом, поддерживаемым многочисленными удостоверяющими центрами.

Тема 10. Экранирование, анализ защищенности. Обеспечение высокой доступности

Формальная постановка задачи экранирования состоит в следующем. Пусть имеется два множества информационных систем. Экран — это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем. Контроль потоков состоит в их фильтрации, возможно, с выполнением некоторых преобразований.

На следующем уровне детализации экран (полупроницаемую мембрану) удобно представлять как последовательность фильтров. Каждый из фильтров, проанализировав данные, может задержать (не пропустить) их. а может и сразу "перебросить" за экран. Кроме того, допускается преобразование данных, передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю.

Экранирование помогает поддерживать доступность сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, вызванную внешней активностью. Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности в ИС организации.

Экранирование может быть частичным, защищающим определенные информационные сервисы. Ограничивающий интерфейс также можно рассматривать как разновидность экранирования. На невидимый объект трудно нападать, особенно с помощью фиксированного набора средств. В этом

смысле Web-интерфейс обладает естественной защитой, особенно в том случае, когда гипертекстовые документы формируются динамически. Каждый пользователь видит лишь то, что ему положено видеть.

Архитектурные аспекты

Бороться с угрозами, присущими сетевой среде, средствами универсальных операционных систем не представляется возможным. Универсальная ОС — это огромная программа, наверняка содержащая, помимо явных ошибок, некоторые особенности, которые могут быть использованы для нелегального получения привилегий. Современная технология программирования не позволяет сделать столь большие программы безопасными. Кроме того, администратор, имеющий дело со сложной системой, далеко не всегда в состоянии учесть все последствия производимых изменений. Наконец, в универсальной многопользовательской системе бреши в безопасности постоянно создаются самими пользователями (слабые и/или редко изменяемые пароли, неудачно установленные права доступа, оставленный без присмотра терминал и т.п.). Единственный перспективный путь связан с разработкой специализированных сервисов безопасности, которые в силу своей простоты допускают формальную или неформальную верификацию. Межсетевой экран как раз и является таким средством, допускающим дальнейшую декомпозицию, связанную с обслуживанием различных сетевых протоколов.

Межсетевой экран — идеальное место для встраивания средств активного аудита. С одной стороны, и на первом, и на последнем защитном рубеже выявление подозрительной активности по-своему важно. С другой стороны, МЭ способен реализовать сколь угодно мощную реакцию на подозрительную активность, вплоть до разрыва связи с внешней средой. Правда, нужно отдавать себе отчет в том, что соединение двух сервисов безопасности в принципе может создать брешь, способствующую атакам на доступность.

На межсетевой экран целесообразно возложить идентификацию/аутентификацию внешних пользователей, нуждающихся в доступе к корпоративным ресурсам (с поддержкой концепции единого входа в сеть).

Ситуации, когда корпоративная сеть содержит лишь один внешний канал, являются скорее исключением, чем правилом. Напротив, типична ситуация, при которой корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к Internet. В этом случае каждое подключение должно защищаться своим экраном. Точнее говоря, можно считать, что корпоративный внешний межсетевой экран является составным, и требуется решать задачу согласованного администрирования (управления и аудита) всех компонентов. Противоположностью составным корпоративным МЭ (или их компонентами) являются персональные межсетевые экраны и персональные экранирующие устройства. Первые являются программными продуктами, которые устанавливаются на персональные компьютеры и защищают только их. Вторые реализуются на отдельных устройствах и защищают небольшую локальную сеть, такую как сеть домашнего офиса.

Классификация межсетевых экранов

При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI. Межсетевые экраны также целесообразно классифицировать по уровню фильтрации — канальному, сетевому, транспортному или прикладному. Соответственно, можно говорить об экранирующих концентраторах (мостах, коммутаторах) (уровень 2), маршрутизаторах (уровень 3), о транспортном экранировании (уровень 4) и о прикладных экранах (уровень 7). Существуют также комплексные экраны, анализирующие информацию на нескольких уровнях.

Фильтрация информационных потоков осуществляется межсетевыми экранами на основе набора правил, являющихся выражением сетевых аспектов политики безопасности организации. В этих правилах, помимо информации, содержащейся в фильтруемых потоках, могут фигурировать данные, полученные из окружения, например, текущее время, количество активных соединений, порт, через который поступил сетевой запрос, и т.д. Таким образом, в межсетевых экранах используется очень мощный логический подход к разграничению доступа.

Экранирующие маршрутизаторы (и концентраторы) имеют дело с отдельными пакетами данных, поэтому иногда их называют пакетными фильтрами. Решения о том, пропустить или задержать

данные, принимаются для каждого пакета независимо, на основании анализа адресов и других полей заголовков сетевого (канального) и, быть может, транспортного уровней. Еще один важный компонент анализируемой информации — порт, через который поступил пакет.

Экранирующие концентраторы являются средством не столько разграничения доступа, сколько оптимизации работы локальной сети за счет организации так называемых виртуальных локальных сетей. Последние можно считать важным результатом применения внутреннего межсетевого экранирования.

Современные маршрутизаторы позволяют связывать с каждым портом несколько десятков правил и фильтровать пакеты как на входе, так и на выходе. В принципе, в качестве пакетного фильтра может использоваться и универсальный компьютер, снабженный несколькими сетевыми картами.

Основные достоинства экранирующих маршрутизаторов — доступная цена (на границе сетей маршрутизатор нужен практически всегда, вопрос лишь в том, как задействовать его экранирующие возможности) и прозрачность для более высоких уровней модели OSI. Основной недостаток — ограниченность анализируемой информации и, как следствие, относительная слабость обеспечиваемой защиты.

Транспортное экранирование позволяет контролировать процесс установления виртуальных соединений и передачу информации по ним. С точки зрения реализации экранирующий транспорт представляет собой довольно простую, а значит, надежную программу.

При использовании прикладных МЭ, помимо фильтрации, реализуется еще один важнейший аспект экранирования. Субъекты из внешней сети видят только шлюзовой компьютер; соответственно, им доступна только та информация о внутренней сети, которую он считает нужным экспортировать. Прикладной МЭ на самом деле экранирует, то есть заслоняет, внутреннюю сеть от внешнего мира. В то же время, субъектам внутренней сети кажется, что они напрямую общаются с объектами внешнего мира. Недостаток прикладных МЭ — отсутствие полной прозрачности, требующее специальных действий для поддержки каждого прикладного протокола.

Комплексность МЭ может достигаться разными способами: "снизу вверх", от сетевого уровня через накопление контекста к прикладному уровню, или "сверху вниз", посредством дополнения прикладного МЭ механизмами транспортного и сетевого уровней.

Помимо выразительных возможностей и допустимого количества правил, качество межсетевого экрана определяется еще двумя очень важными характеристиками - простотой использования и собственной защищенностью. В плане простоты использования первостепенное значение имеют наглядный интерфейс при определении правил фильтрации и возможность централизованного администрирования составных конфигураций. В свою очередь, в последнем аспекте хотелось бы выделить средства централизованной загрузки правил фильтрации и проверки набора правил на непротиворечивость. Важен и централизованный сбор и анализ регистрационной информации, а также получение сигналов о попытках выполнения действий, запрещенных политикой безопасности.

Собственная защищенность межсетевого экрана обеспечивается теми же средствами, что и защищенность универсальных систем. Имеется в виду физическая защита, идентификация и аутентификация, разграничение доступа, контроль целостности, протоколирование и аудит. При выполнении централизованного администрирования следует также позаботиться о защите информации от пассивного и активного прослушивания сети, то есть обеспечить ее (информации) целостность и конфиденциальность. Крайне важно оперативное наложение заплат, ликвидирующих выявленные уязвимые места МЭ.

Хотелось бы подчеркнуть, что природа экранирования как сервиса безопасности очень глубока. Помимо блокирования потоков данных, нарушающих политику безопасности, межсетевой экран может скрывать информацию о защищаемой сети, тем самым затрудняя действия потенциальных злоумышленников. Мощным методом сокрытия информации является трансляция "внутренних" сетевых адресов, которая попутно решает проблему расширения адресного пространства, выделенного организации.

Анализ защищенности

Сервис анализа защищенности предназначен для выявления уязвимых мест с целью их оперативной ликвидации. Сам по себе этот сервис ни от чего не защищает, но помогает обнаружить (и устранить) пробелы в защите раньше, чем их сможет использовать злоумышленник. В первую очередь, имеются в виду не архитектурные (их ликвидировать сложно), а "оперативные" бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения.

Системы анализа защищенности (называемые также сканерами защищенности), как и рассмотренные выше средства активного аудита, основаны на накоплении и использовании знаний.

В принципе, могут выявляться бреши самой разной природы: наличие вредоносного ПО (в частности, вирусов), слабые пароли пользователей, неудачно сконфигурированные операционные системы, небезопасные сетевые сервисы, неустановленные заплаты, уязвимости в приложениях и т.д. Однако наиболее эффективными являются сетевые сканеры (очевидно, в силу доминирования семейства протоколов TCP/IP), а также антивирусные средства. Антивирусную защиту мы причисляем к средствам анализа защищенности, не считая ее отдельным сервисом безопасности.

Сканеры могут выявлять уязвимые места как путем пассивного анализа, то есть изучения конфигурационных файлов, задействованных портов и т.п., так и путем имитации действий атакующего. Некоторые найденные уязвимые места могут устраняться автоматически (например, лечение зараженных файлов), о других сообщается администратору.

Обеспечение высокой доступности

Информационная система предоставляет своим пользователям определенный набор услуг (сервисов). Говорят, что обеспечен нужный уровень доступности этих сервисов, если следующие показатели находятся в заданных пределах:

Эффективность услуг. Эффективность услуги определяется в терминах максимального времени обслуживания запроса, количества поддерживаемых пользователей и т.п. Требуется, чтобы эффективность не опускалась ниже заранее установленного порога.

Время недоступности. Если эффективность информационной услуги не удовлетворяет наложенным ограничениям, услуга считается недоступной. Требуется, чтобы максимальная продолжительность периода недоступности и суммарное время недоступности за некоторой период (месяц, год) не превышали заранее заданных пределов.

Задачу обеспечения высокой доступности необходимо решать для современных конфигураций, построенных в технологии клиент/сервер. Это означает, что в защите нуждается вся цепочка — от пользователей (возможно, удаленных) до критически важных серверов (в том числе серверов безопасности).

Основные угрозы доступности были рассмотрены нами ранее.

В соответствии с ГОСТ 27.002, под отказом понимается событие, которое заключается в нарушении работоспособности изделия. В простейшем случае можно считать, что отказы любого компонента составного изделия ведут к общему отказу, а распределение отказов во времени представляет собой простой пуассоновский поток событий. В таком случае вводят понятие интенсивности отказов и среднего времени наработки на отказ, которые связаны между собой соотношением

$$T_i = \frac{1}{\lambda_i}$$

где i — номер компонента, λ_i — интенсивность отказов, T_i — среднее время наработки на отказ.

Интенсивности отказов независимых компонентов складываются:

$$\lambda = \lambda_1 + \ldots + \lambda_n$$

а среднее время наработки на отказ для составного изделия задается соотношением

$$T = \frac{1}{\lambda}$$

Пуассоновская модель позволяет обосновать еще одно очень важное положение, состоящее в том, что эмпирический подход к построению систем высокой доступности не может быть реализован за приемлемое время. При традиционном цикле тестирования/отладки программной систе-

мы по оптимистическим оценкам каждое исправление ошибки приводит к экспоненциальному убыванию (примерно на половину десятичного порядка) интенсивности отказов. Отсюда следует, что для того, чтобы на опыте убедиться в достижении необходимого уровня доступности, независимо от применяемой технологии тестирования и отладки, придется потратить время, практически равное среднему времени наработки на отказ.

Пуассоновская модель применима в тех случаях, когда информационная система содержит одиночные точки отказа, то есть компоненты, выход которых из строя ведет к отказу всей системы. Для исследования систем с резервированием применяется иной формализм.

В качестве меры доступности можно принять вероятность приемлемости эффективности услуг, предоставляемых информационной системой, на всем протяжении рассматриваемого отрезка времени. Чем большим запасом эффективности располагает система, тем выше ее доступность.

Основы мер обеспечения высокой доступности

Основой мер повышения доступности является применение структурированного подхода, нашедшего воплощение в объектно-ориентированной методологии. Структуризация необходима по отношению ко всем аспектам и составным частям информационной системы — от архитектуры до административных баз данных, на всех этапах ее жизненного цикла — от инициации до выведения из эксплуатации. Структуризация, важная сама по себе, является одновременно необходимым условием практической реализуемости прочих мер повышения доступности. Только маленькие системы можно строить и эксплуатировать как угодно, у больших систем свои законы.

Главное при разработке и реализации мер обеспечения высокой доступности — полнота и систематичность. В этой связи представляется целесообразным составить (и поддерживать в актуальном состоянии) карту информационной системы организации (на что мы уже обращали внимание), в которой фигурировали бы все объекты ИС, их состояние, связи между ними, процессы, ассоциируемые с объектами и связями. С помощью подобной карты удобно формулировать намечаемые меры, контролировать их исполнение, анализировать состояние ИС.

Отказоустойчивость и зона риска

Информационную систему можно представить в виде графа сервисов, ребра в котором соответствуют отношению "сервис А непосредственно использует сервис В".

Пусть в результате осуществления некоторой атаки (источником которой может быть как человек, так и явление природы) выводится из строя подмножество сервисов S_1 (то есть эти сервисы в результате нанесенных повреждений становятся неработоспособными). Назовем S_1 зоной поражения. В зону риска S мы будем включать все сервисы, эффективность которых при осуществлении атаки падает ниже допустимого предела. Очевидно, S_1 — подмножество S. S строго включает S_1, когда имеются сервисы, непосредственно не затронутые атакой, но критически зависящие от пораженных, то есть неспособные переключиться на использование эквивалентных услуг либо в силу отсутствия таковых, либо в силу невозможности доступа к ним. Например, зона поражения может сводиться к одному порту концентратора, обслуживающему критичный сервер, а зона риска охватывает все рабочие места пользователей сервера.

Чтобы система не содержала одиночных точек отказа, то есть оставалась "живучей" при реализации любой из рассматриваемых угроз, ни одна зона риска не должна включать в себя предоставляемые услуги. Нейтрализацию отказов нужно выполнять внутри системы, незаметно для пользователей, за счет размещения достаточного количества избыточных ресурсов.

Обеспечение отказоустойчивости

Основным средством повышения "живучести" является внесение избыточности в конфигурацию аппаратных и программных средств, поддерживающей инфраструктуры и персонала, резервирование технических средств и тиражирование информационных ресурсов (программ и данных). Меры по обеспечению отказоустойчивости можно разделить на локальные и распределенные. Локальные меры направлены на достижение "живучести" отдельных компьютерных систем или их аппаратных и программных компонентов (в первую очередь с целью нейтрализации внутренних отказов ИС).

Аппаратура — относительно статичная составляющая, однако было бы ошибкой полностью отказывать ей в динамичности. В большинстве организаций информационные системы находятся в постоянном развитии, поэтому на протяжении всего жизненного цикла ИС следует соотносить все изменения с необходимостью обеспечения "живучести", не забывать "тиражировать" новые и модифицированные компоненты.

Программы и данные более динамичны, чем аппаратура, и резервироваться они могут постоянно, при каждом изменении, после завершения некоторой логически замкнутой группы изменений или по истечении определенного времени.

Выделим следующие классы тиражирования:

Симметричное/асимметричное. Тиражирование называется симметричным, если все серверы, предоставляющие данный сервис, могут изменять принадлежащую им информацию и передавать изменения другим серверам. В противном случае тиражирование называется асимметричным.

Синхронное/асинхронное. Тиражирование называется синхронным, если изменение передается всем экземплярам сервиса в рамках одной распределенной транзакции. В противном случае тиражирование называется асинхронным.

Осуществляемое средствами сервиса, хранящего информацию/внешними средствами.

Асинхронное тиражирование может производиться на сервер, работающий в режиме "горячего" резерва, возможно, даже обслуживающего часть пользовательских запросов, или на сервер, работающий в режиме "теплого" резерва, когда изменения периодически "накатываются", но сам резервный сервер запросов не обслуживает.

Достоинство "теплого" резервирования в том, что его можно реализовать, оказывая меньшее влияние на основной сервер. Это влияние вообще может быть сведено к нулю, если асинхронное тиражирование осуществляется путем передачи инкрементальных копий с основного сервера (резервное копирование необходимо выполнять в любом случае).

Основной недостаток "теплого" резерва состоит в длительном времени включения, что может быть неприемлемо для "тяжелых" серверов, таких как кластерная конфигурация сервера СУБД. Здесь необходимо проводить измерения в условиях, близких к реальным.

Второй недостаток "теплого" резерва вытекает из опасности малых изменений. Может оказаться, что в самый нужный момент срочный перевод резерва в штатный режим невозможен.

Учитывая приведенные соображения, следует в первую очередь рассматривать возможность "горячего" резервирования, либо тщательно контролировать использование "теплого" резерва и регулярно (не реже одного раза в неделю) проводить пробные переключения резерва в "горячий" режим.

Программное обеспечение промежуточного слоя

С помощью программного обеспечения промежуточного слоя (ПО ПС) можно для произвольных прикладных сервисов добиться высокой "живучести" с полностью прозрачным для пользователей переключением на резервные мощности.

Перечислим основные достоинства ПО ПС, существенные для обеспечения высокой доступности.

- ПО ПС уменьшает сложность создания распределенных систем. Подобное ПО берет на себя часть функций, которые в локальном случае выполняют операционные системы;
- ПО ПС берет на себя маршрутизацию запросов, позволим тем самым обеспечить "живучесть" прозрачным для пользователей образом;
- ПО ПС осуществляет балансировку загрузки вычислительный мощностей, что также способствует повышению доступности данных;
- ПО ПС в состоянии осуществлять тиражирование любой им формации, а не только содержимого баз данных. Следовательно, любое приложение можно сделать устойчивым к отказам серверов;
- ПО ПС в состоянии отслеживать состояние приложений и при необходимости тиражировать и перезапускать программы, что гарантирует "живучесть" программных систем;

ПО ПС дает возможность прозрачным для пользователей образом выполнять переконфигурирование (и, в частности, наращивание) серверных компонентов, что позволяет масштабировать систему, сохраняя инвестиции в прикладные системы.

Обеспечение обслуживаемости

Меры по обеспечению обслуживаемости направлены на снижение сроков диагностирования и устранения отказов и их последствий.

Для обеспечения обслуживаемости рекомендуется соблюдать следующие архитектурные принципы:

- ориентация на построение информационной системы из унифицированных компонентов с целью упрощения замены отказавших частей;
- ориентация на решения модульной структуры с возможностью автоматического обнаружения отказов, динамического переконфигурирования аппаратных и программных средств и замены отказавших компонентов в "горячем" режиме.

Динамическое переконфигурирование преследует две основные цели:

- изоляция отказавших компонентов;
- сохранение работоспособности сервисов.

Изолированные компоненты образуют зону поражения реализованной угрозы. Чем меньше соответствующая зона риска, тем выше обслуживаемость сервисов. Так, при отказах блоков питания, вентиляторов и/или дисков в современных серверах зона риска ограничивается отказавшим компонентом; при отказах процессорных модулей весь сервер может потребовать перезагрузки (что способно вызвать дальнейшее расширение зоны риска). Очевидно, в идеальном случае зоны поражения и риска совпадают, и современные серверы и активное сетевое оборудование, а также программное обеспечение ведущих производителей весьма близки к этому идеалу.

Возможность удаленного выполнения административных действий — важное направление повышения обслуживаемости, поскольку при этом ускоряется начало восстановительных мероприятий, а в идеале все работы (обычно связанные с обслуживанием программных компонентов) выполняются в удаленном режиме, без перемещения квалифицированного персонала, то есть с высоким качеством и в кратчайшие сроки. Для современных систем возможность удаленного администрирования — стандартное свойство, но важно позаботиться о его практической реализуемости в условиях разнородности конфигураций (в первую очередь клиентских). Централизованное распространение и конфигурирование программного обеспечения, управление компонентами информационной системы и диагностирование — надежный фундамент технических мер повышения обслуживаемости.

Цель мероприятий в области информационной безопасности — защитить интересы субъектов информационных отношений. Интересы эти многообразны, но все они концентрируются вокруг трех основных аспектов:

- доступность;
- целостность;
- конфиденциальность.

Первый шаг при построении системы ИБ организации — ранжирование и детализация этих аспектов.

Важность проблематики ИБ объясняется двумя основными причинами:

- ценностью накопленных информационных ресурсов;
- критической зависимостью от информационных технологий.

Разрушение важной информации, кража конфиденциальных данных, перерыв в работе вследствие отказа — все это выливается в крупные материальные потери, наносит ущерб репутации организации. Проблемы с системами управления или медицинскими системами угрожают здоровью и жизни людей.

Современные информационные системы сложны и, значит, опасны уже сами по себе, даже без учета активности злоумышленников. Постоянно обнаруживаются новые уязвимые места в программном обеспечении. Приходится принимать во внимание чрезвычайно широкий спектр аппаратного и программного обеспечения, многочисленные связи между компонентами.

Проблема ИБ — не только (и не столько) техническая; без законодательной базы, без постоянного внимания руководства организации и выделения необходимых ресурсов, без мер управления персоналом и физической защиты решить ее невозможно. Комплексность также усложняет проблематику ИБ; требуется взаимодействие специалистов из разных областей.

Миссия обеспечения информационной безопасности трудна, во многих случаях невыполнима, но всегда благородна.

3. 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:

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

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 $\mathbf{L}_1 = 10\,lg\mathbf{I} + 120$ - 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) элементов 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:

$\mathbf{Q}_{пер}$, дБ = 12,5***lg***ρ + 14 (3)

для стен с $\rho < 200$ кг/м^2;

$\mathbf{Q}_{пер}$, дБ = 14,5***lg***ρ +15 (4)

для стен с $\rho > 200$ кг/м^2;

$\mathbf{Q}_{пер}$, дБ = 14***lg*** $(\rho_1\rho_1)$+20 ***lg***δ-13 (5)

для двойных жестких перегородок с воздушной прослойкой между ними с поверхностной плотностью ρ = 30...100 кг/м^2; где ρ1 и ρ1 - 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
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		-8	0,040	9	0,50	26	0,960
		-7	0,050	12	0,60	27	0,970
w = 0		-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	4000	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					
		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
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
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
	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.

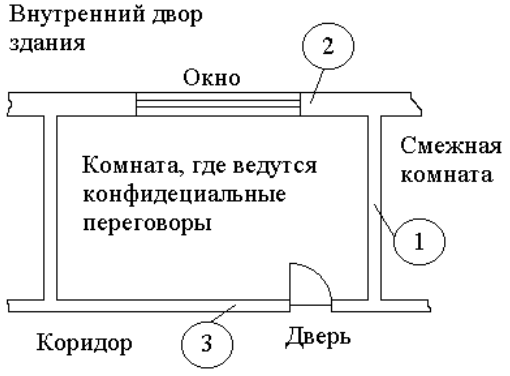


Рис. 1. Схема исследуемого кабинета

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*(1,34х0,095 + +2,5х0,075 + 4,24х0,06 + 5,88х0,004) = 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**о/(**S**1 + **S**о))*($10^{0,1(\mathbf{Q}1-\mathbf{Q}о)}$-1)],

где **Q**1 = 59 дБ;

Qо = 38 дБ;

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

где **Q**1 = 48 дБ;

Qо = 18 дБ;

(**S**о/(**S**1 + **S**о)) = 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 **Е**ф определяется из выражения:

Еф= **L**р – **L**ш.

№ октавы	Ср. частота, *f*р	**L**2 = **L**р, дБ	Предельные спектры шумов ПС-40, **L**ш, дБ	**Е**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*(1,34х0,4 + 2,5х0,35 + +4,24х0,3 + 5,88х0,25 + 5,0х0,05 + 1,04х0,03) = 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 варианта	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)
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%	Стена (табл. 7, п. 1.35) Дверь (табл. 7, п. 3.3) **S**o = 30%

Номер варианта	1. Смежное помещение	2. Наружная стена	3. Коридор
		ПС-40 (табл. 1)	**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% **ПС**-35 (табл. 1)	Стена (табл. 7, п. 1.40) Дверь (табл. 7, п. 3.8) **S**o = 20% **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);

$\boldsymbol{f}_{экв}$ -ширина полосы пропускания приемника (Гц);

$\boldsymbol{T}_a$ - эквивалентная шумовая температура, характеризующая интенсивность помех;

$\boldsymbol{T}_o = 273^oK$.

Ширина полосы пропускания приемника $\boldsymbol{f}_{экв}$ 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 $\mathbf{T}_a = 293^oK$, $\boldsymbol{f}_{экв}$=40 Мгц расчитаем среднеквадратическую напряженность поля $\mathbf{E}_a$:

на частоте 100 Мгц - $\mathbf{E}_a$ = -9,2 дБ (0,346 мкВ/м);

на частоте 500 Мгц - $\mathbf{E}_a$ = 4,8 дБ (1,738 мкВ/м);

на частоте 1000 Мгц - $\mathbf{E}_a$ = 10,8 дБ (3,467 мкВ/м).

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

$$\mathbf{k}_з = 1 / \mathbf{r}^n, \qquad (2)$$

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:

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

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):

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

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 ($2Q/N_O$) возрастает в **n** (количество повторений) раз по сравнению с отношением сигнал/помеха на входе приемника при однократном отсчете, т.е.:

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

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

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

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

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

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.

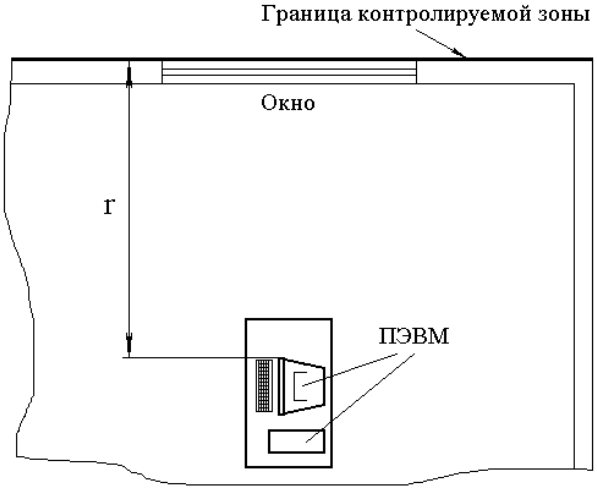


Рис. 2. Схема помещения для проведения расчетов

Таблица 2

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

Номер	Значения электромагнитного поля **E** (мкВ/м) на частотах

п/п			
	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 формуле $\Delta = \mathbf{E}_{кз} / \mathbf{E}_а$	0,999≈1	0,79	0,51

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 $\mathbf{E}_а$ атмосферных помех не расчитывать, считать одинаковыми для всех вариантов и равными:

	100 МГц	500 МГц	1000 МГц
$\mathbf{E}_а$, мкВ/м ($\mathbf{T}_а$=293°K, fэкв=40 Мгц)	0,346	1,738	3,467

Варианты:

Номер варианта	$\mathbf{k}_з = 1 / \mathbf{r}^n$		$\mathbf{k}_{экр}$ 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

Лабораторная работа 3. ИЗУЧЕНИЕ ТРАДИЦИОННЫХ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ.ШИФРЫ ПЕРЕСТАНОВКИ

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.

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.

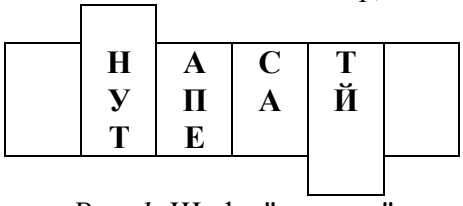


Рис. 1. Шифр "скитала"

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**

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**

И	Р	Ы	С	О	О	Ь

До перестановки

О	Р	С	О	Ы	Ь	И

После 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**

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

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

Исходная таблица Перестановка столбцов Перестановка строк

Рис. 4. Пример выполнения шифрования методом двойной перестановки

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

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. 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**

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. ПРИНИМАЛА ЕГО УЧИТЕЛЬНИЦА, ТВЕРДО УВЕРЕННАЯ В МОИХ ГЛУБОКИХ ПОЗНАНИЯХ В ЭТОЙ ОБЛАСТИ	СЕРПОВИЩЕ
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 ДРУГОЙ	КОНЦЕПЦИЯ
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

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.

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.

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.

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.

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

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

Задание

1. Зашифровать текст при помощи таблицы Вижинера (см. рис. 4), используя ключевое слово.

2. 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	ПАРТНЕР

Номер варианта	Текст	Ключевое слово
	ТЕКСТ, А ПОРЯДОК СИМВОЛОВ	
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
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)

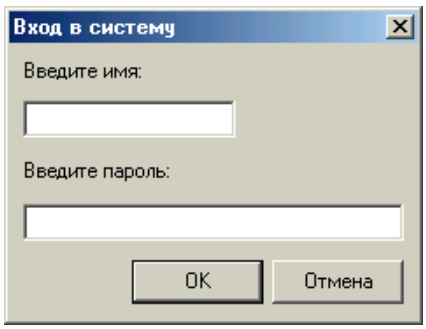
Длина не меньше минимальной длины, устанавливаемой администратором и сохраняемой в учетной записи пользователя.

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.

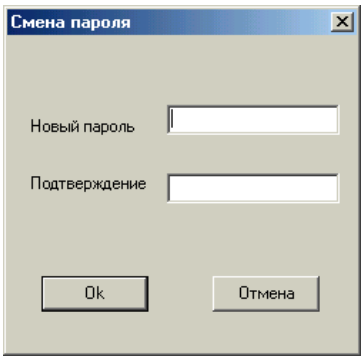
Возможный вид диалоговых форм программы

Окно входа в программу



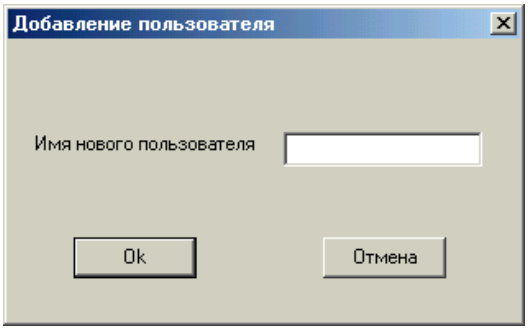
Может быть создано на основе шаблона Password Dialog, выбираемого с помощью команды File | New | Dialogs систем программирования Borland Delphi или Borland C++ Builder.

Окно смены пароля



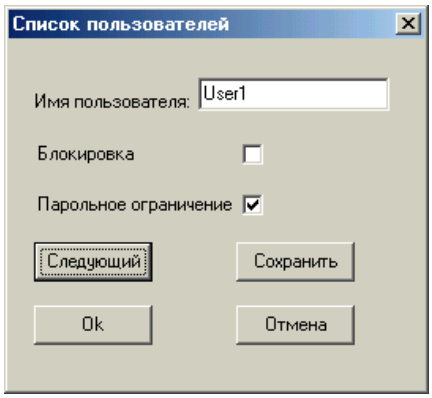
Возможно добавление на форму надписи «Старый пароль» и редактируемой строки для ввода действующего пароля.

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 отчета 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?

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

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

1. В процессе чтения лекционного курса (ключевые лекции) рекомендуется проводить фронтальный опрос, начиная со второй лекции, задавая вопросы студентам по содержанию предыдущей лекции для проверки усвоения лекционного материала.

2. На лекционных занятиях рекомендуется использовать наглядность в виде слайд-презентаций.

3. При подготовке к лабораторным занятиям приветствуется поиск информации в ИНТЕРНЕТ.

6. КОМПЛЕКТ ЭКЗАМЕНАЦИОННЫХ БИЛЕТОВ

Экзаменационные билеты для студентов включают два теоретических вопроса. Вопросы к экзамену выдаются студентам на последней лекции. Примерный комплект экзаменационных билетов выглядит следующим образом.

АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Утверждено на заседании кафедры
_____
Заведующий кафедрой
Утверждаю:_____

Кафедра___ИУС___
Факультет___МиИ_
Курс __5_____
Дисциплина_ИБиЗИ__

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 __5_____
Дисциплина_ИБиЗИ__

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 __5_____
Дисциплина_ЗИ__

Экзаменационный билет №__3___

1. Основные механизмы и сервисы безопасности.
2. Программно-технические меры обеспечения ИБ, виды, архитектурные принципы, сервисы.