МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Забайкальский государственный университет»
(ФГБОУ ВО ЗабГУ)
Кафедра Физики и техники связи

Методические указания к лабораторным и практическим работам по дисциплине

«Основы защиты сетей и систем связи»

»

Чита, 2014

ОГЛАВЛЕНИЕ

ОБЩИЕ СВЕДЕНИЯ

Защиту информации в настоящее время необходимо рассматривать как часть интегрированной системы безопасности. Актуальность вопросов защиты информации обусловлена двумя обстоятельствами: первое – современные системы охранной безопасности, применяемые для противодействия проникновениям на объекты собственности являются сложными информационно-телекоммуникационными системами, базирующимися на современных информационных технологиях; второе – информация, хранящаяся и обрабатываемая на охраняемых объектах, также является объектом охраны.

В условиях рынка информация приобретает особую ценность и становится товаром, нередко информацию получают в результате коммерческой разведки. Противоправные действия осуществляются с использованием всех достижений современной микроэлектроники: приемников, передатчиков, усилителей, ретрансляторов, магнитофонов, телекамер, компьютеров и т.п. С помощью данных средств подслушивают, подсматривают, перехватывают и записывают сообщения, нередко искажают и уничтожают чужую информацию. Современные электронные приборы позволяют проконтролировать практически все используемые каналы сбора, обработки и передачи информации – акустический канал, телефон, радио, компьютер и т.д.

Необходимость практической подготовки специалистов по защите информации в рамках лабораторных практикумов становится очевидной.

Данное учебное пособие предназначено для подготовки студентов, обучающихся по направлению 090100 – «Информационная безопасность». Пособие построено в соответствии с темами теоретического цикла дисцип-лины «Основы информационной безопасности».

Лабораторные работы выполняются на базе следующих программных, программно-аппаратных, технических и криптографических средств: САЗ ВОЛНА-3М, ПАК СЗИ от НСД «Аккорд-АМДЗ», возможных программ восстановления: EasyRecovery, Filerecovery, Recover4all, возможных программ гарантированного удаления: Acronis Privacy Expert Suite, Acronis Drive Cleanser, Systerac XP Toolls Shreder, Paragon Disc Wiper и возможных про-грамм обеспечения целостности: Tripwire ASR, Symantec Enterprise Security Manager, IBM Tivoli Business Service Manager, Аккорд, ФПСУ X25 ACCESS TM-SHELL и др..

ЛАБОРАТОРНАЯ РАБОТА № 1

Тема: Виды информации и основные методы ее защиты.

Цель работы

Применение основ информационной безопасности для имитации действий нарушителя по раскрытию (нарушению конфиденциальности) при использовании одного и того же одноразового блокнота (гаммы) на основе побитового сложения по модулю 2 (взлом двухразового блокнота).

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Изучить соответствующий теоретический материал по курсу «Программирование».
3. Написать на языке Си программу, реализующую поставленную задачу.
4. Проанализировать проделанную работу и предложить свой метод противодействия реализованной атаке.
5. Результат отразить в отчете.

Краткие теоретические сведения

Безопасность для различных сфер жизнедеятельности личности, общества и государства опирается на понятие ограничения доступа к информации. Шифрование используется как метод усиления таких свойств качественной информации, как конфиденциальность и целостность. Можно легко получить не раскрываемый шифр, но тут имеется одна тонкость. Сначала нужно найти процесс, который может генерировать произвольную бесконечную строку битов, которая называется гаммой. Во-вторых, необходимо преобразовать открытый текст в битовую строку и вычислить побитовое сложение по модулю 2 (операция XOR) открытого текста и ключевой строки. После чего можно послать результирующий зашифрованный текст получателю по незащищенному каналу. Шифрованный текст не может быть раскрыт, поскольку каждая возможная ключевая строка является одинаково вероятным кандидатом; нарушитель не имеет информации. Дополнительно к посылке шифро-

ванного текста отправитель передает ключевую строку по защищенному каналу получателю так, что получатель может расшифровать текст, обрабаты-вая XOR шифрованного текста и ключевой строки. Хитрость состоит в том, что нам нужно иметь защищенный канал для посылки ключевой строки.

Более практичный подход для отправителя: сгенерировать эту ключевую строку заранее. Например, отправитель может создать 1000 компакт-дисков, полных произвольных битов, и переправить их получателю на БТР.

Хотя еженедельная посылка 1000 дисков и является широкополосной операцией, у нее есть один изъян: ключевой поток должен быть такой же длины, как и данные; если данные на один бит длиннее, чем ожидалось, то появятся проблемы. Строки однократного использования используются иногда на практике (например, однократные пароли).

Обходной путь, часто применяющийся на практике, должен выбрать короткий ключ (скажем, 64 бита) и использовать псевдослучайный генератор чисел, чтобы генерировать ключевую строку из короткого ключа. Теперь нужно послать только 64 бита по защищенному каналу, но придется пола-гаться на некоторое искусство. А именно: нужен хороший псевдослучайный генератор, для которого по выходу нельзя догадаться о ключе, и для которого один и тот же выход всегда генерируется из данного короткого ключа. Но ес-ли нарушитель может управлять входом, то он может восстановить выход произвольного генератора и, возможно, угадать будущие случайные числа! Из этого следует, что трудно разработать хороший псевдослучайный генера-тор. Поэтому нужны альтернативные способы шифрования.

Можно ли вычислить, какие два документа зашифровал Борис, используя один и тот же одноразовый блокнот (гамму) – побитовое сложение по модулю 2 (и что собой представляет этот одноразовый блокнот)?

Известна следующая информация:

1. Шифрование использует коды ASCII со 128 возможными символами в любой позиции (хотя некоторые – значительно более вероятны, чем другие).
2. Используемый одноразовый блокнот был произведён псевдослучайным образом, со значениями в пределах от 0 до 127.
3. Использовался один и тот же блокнот, чтобы зашифровать оба исходных текста.

4. Если длины исходных текстов не совпадают, то более короткий из них дополняется пробелами.
5. Эти тексты - части относительно известных текстов на английском языке.

Шифр 1:

42 102 120 61 61 67 57 84 117 66 41 33 100 116 15 55 80 16 120 0 54
78 105 113 96 25 43 69 39 82 125 40 40 24 120 94 92 37 114 53 64 63
107 19 82 62 99 81 81 69 103 22 120 123 71 1 113 57 5 50 67 40 2 85
67 11 40 56 22 89 127 95 59 121 27 121 95 121 114 3 1 5 45 103 112
127 62 34 39 13 44 30 80 19 2 60 72 80 56 18 93 31 69 66 45 122 71
33 58 113 12 120 50 63 39 5 110 28 14 48 109 10 68 95 92 88 0 30 107
4 54 92 104 122 5 95 15 118 42 93 75 83 9 35 106 8 13 53 101 93 32
60 53 36 72 101 121 121 121 99 98 89 30 71 87 87 14 107 28 36 42 108
98 95 99 68 2 60

Шифр 2:

34 40 111 117 37 64 32 88 55 74 112 117 103 121 23 54 91 5 116 84 42
79 127 35 114 80 48 67 39 71 53 62 97 12 113 48 47 34 122 57 80 63
122 77 61 93 119 68 71 83 107 87 116 115 2 19 101 112 86 127 78 109 2
89 81 17 85 5 21 94 127 84 59 109 13 42 25 116 126 7 7 18 106 118
113 62 37 63 43 102 69 73 79 14 7 105 70 17 18 25 93 56 7 27 7 84
8 117 50 123 9 44 42 50 98 76 111 6 4 48 117 7 86 88 92 75 29 16
121 65 52 80 107 50 19 8 41 46 10 84 74 95 93 57 106 27 72 125 101
73 97 56 58 51 89 101 108 125 112 99 114 72 18 9 84 30 7 107 89 34
39 103 33 86 36 3 74 104

Программа должна без потерь расшифровывать приведенные файлы (включая список опечаток). Дополнительным заданием может служить соз-дание программы, которая генерирует зашифрованные тексты по заданным открытым текстам.

Содержание отчета

Отчет должен содержать:

1. Описание атаки.
2. Алгоритм, функциональная схема и функциональный состав программы.

3. Вывод, в котором предлагаются методы решения проблемы повторного использования одноразового блокнота.

Контрольные вопросы

1. Кратко сформулируйте виды безопасности для соответствующих сфер жизнедеятельности личности, общества и государства.
2. В чем состоят источники угроз интересам личности?
3. В чем состоят источники угроз интересам общества?
4. В чем состоят источники угроз интересам государства?
5. Перечислите виды информации и основные методы ее защиты.
6. В чем состоят национальные интересы Российской Федерации в информационной сфере и их что собой представляет их обеспечение.
7. Раскройте понятие информационно-безопасного шифрования.
8. В чем состоит сложность использования симметричных криптографических систем?
9. В чем заключаются слабости решения с помощью псевдослучайных генераторов чисел?
10. Приведите несколько примеров применения одноразовых блокнотов.
11. Расскажите о методах противодействия данной атаке.

ЛАБОРАТОРНАЯ РАБОТА № 2

Тема: Виды угроз информационной безопасности Российской Федерации.

Цель работы

Применение основ информационной безопасности для нахождения путей противодействия угрозе раскрытия (нарушения конфиденциальности) при наличии дискреционной модели доступа путем реализации модели типовой атаки «Троянский конь» в ОС Novell Netware 4.12.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».

2. Изучить теоретический материал по курсу «Программирование» на тему «Работа с файлами».
3. Создать объекты атаки, используя утилиту SYSCON ОС Novell Netware 4.12.
4. Написать на языке Си программу, реализующую атаку типа «Троянский конь».
5. Проанализировать проделанную работу и предложить свой метод противодействия реализованной атаке.
6. Результат отразить в отчете.

Краткие теоретические сведения

В системах ГМУ широко применяются системы безопасности, основанные на моделях. Модели безопасности рассматриваются в соответствии с типом угроз, от которых защищают информацию вычислительные системы, разработанные на основе данных моделей. Модель разграничения доступа защищает от угрозы раскрытия информации, заключающейся в том, что ин-формация становится известной посторонним. Естественной основой для по-строения политики разграничения доступа является модель, построенная по принципу разграничения прав. Основными типами моделей, построенных на предоставлении прав, являются модели дискреционного и мандатного доступа.

К достоинствам модели дискреционного доступа можно отнести хорошую гранулированность защиты и относительно простую реализацию. В качестве примера реализации можно привести матрицу доступа, строки которой соответствуют субъектам системы, а столбцы – объектам; элементы матрицы характеризуют права доступа.

К недостаткам модели дискреционного доступа относится проблема троянских программ (троянских коней). Троянскую программу следует определять как любую программу, от которой ожидается выполнение желаемого действия, а она на самом деле выполняет какое-нибудь неожиданное или нежелательное действие. Для понимания ее работы необходимо помнить, что при вызове программы на компьютере в системе инициируется последовательность операций, зачастую скрытых от пользователя. Эти операции обычно управляются операционной системой. Троянские программы рассчитаны на то, что когда пользователь инициирует такую последовательность, он

обычно верит в то, что система произведет ее, как полагается. При этом на-рушитель может написать версию троянской программы, которая будучи за-пущенной от имени пользователя-жертвы, передаст его информацию пользо-вателю-нарушителю.

В системе с дискреционной моделью доступа существуют субъекты и объекты. Субъекты – это пользователи, инициирующие процессы (запись и чтение) операционной системы для доступа к объектам. Объекты – ресурсы операционной системы – файлы и каталоги. Для реализации атаки «Троянский конь» в ОС Novell Netware 4.12 необходимо создать два каталога, соответствующих различным уровням секретности (например, SECRET и NONSEC). Создать двух пользователей, имеющих права над данными каталогами:

- Пользователь А имеет права на чтение и запись в каталог SECRET, а также права на запись в каталог NONSEC.
- Пользователь В имеет права на чтение и запись в каталог NONSEC.

Примечание

- Права, определенные над каталогом, совпадают с правами над его содержимым.
- Пользователь А имеет право запускать программы из каталога NONSEC.

Пользователь В в такой системе может реализовать атаку типа «Троянский конь» для раскрытия секретной информации пользователя А. Пусть пользователь А создал файл SECRET.TXT в каталоге SECRET. Тогда в соответствии с расставленными масками прав пользователь А имеет право читать этот файл, а пользователь В – нет. Задачей пользователя В является раскрытие содержимого файла SECRET.TXT. Он создает троянскую программу с безобидным названием GAME.EXE и помещает ее в каталог NONSEC. Затем пользователь В ждет, пока пользователь А не запустит эту программу, которая должна в фоновом режиме копировать файл SECRET.TXT из каталога SECRET в каталог NONSEC. Копирование возможно, так как это действие аналогично записи и не противоречит маске прав пользователя А. Таким образом, содержимое секретного файла SECRET.TXT становится известным несекретному пользователю. Атака завершена. Она останется незамеченной, если действия троянской программы будут замаскированы.

Троянская программа должна без потерь копировать файлы произвольной длины и любым расширением. Дополнительным заданием может служить создание программы, которая делала бы точную копию системы каталогов пользователя А.

Содержание отчета

1. Описание атаки.
2. Алгоритм, функциональная схема и функциональный состав программы.
3. Вывод, в котором предлагаются методы решения проблемы троянского коня.

Контрольные вопросы

1. Перечислите виды угроз безопасности информационного общества.
2. В чем заключается угроза раскрытия информации? Какие еще угрозы Вы знаете?
3. Что положено в основу дискреционной модели доступа?
4. Раскройте понятие троянской программы в контексте защиты информации в вычислительной системе.
5. Какова роль субъектов и объектов в операционной системе?
6. Какие средства позволяют реализовать дискреционную модель доступа в ОС Novell Netware 4.12 (Windows 2000, XP)?
7. Приведите несколько примеров внедрения троянской программы.
8. Как замаскировать действие троянской программы?
9. Расскажите о методах противодействия данной атаке.
10. Какие недостатки присущи дискреционной модели помимо проблемы троянского коня?

ЛАБОРАТОРНАЯ РАБОТА № 3

Тема: Источники угроз информационной безопасности Российской Федерации.

Цель работы

Применение основ информационной безопасности для нахождения путей противодействия угрозе раскрытия (нарушения конфиденциальности) в

мандатной модели доступа при наличии пары: нарушитель – высокоуровневый сообщник.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Написать на языке Си программу, реализующую модель монитора обращений, согласующуюся с мандатной моделью доступа.
3. Проанализировать проделанную работу и предложить свой метод проти-водействия угрозе раскрытия (нарушения конфиденциальности) в данной модели доступа.
4. Результат отразить в отчете.

Краткие теоретические сведения

В системе с мандатной моделью доступа существуют принципалы и объекты. Принципалы – это субъекты аутентификации и ответственности. Они представляют сущности, которые используют информацию, хранящую-ся в объектах. Принципал информации обычно соответствует сотруднику вне компьютерной системы (иными словами, имеет учетную запись в данной компьютерной среде). Объекты – ресурсы операционной системы – файлы и каталоги.

В отличие от дискреционного, мандатный доступ накладывает ограничения на передачу информации от одного пользователя к другому. Это позволяет разрешить проблему троянских коней.

Для большей конкретности рассмотрим предприятие с тремя уровнями секретности:

– общим (пресс-релизы);
– для служебного пользования (телефонный справочник предприятия);
– конфиденциальным (производственный план).

Каждый файл в компьютерной системе помечен меткой конфиденциальности в данной классификации.

Каждый пользователь, имеющий доступ к компьютерной системе, получает допуск на определенный уровень. Высшие исполнительные сотрудники и руководство имеют допуск на 1, 2 и 3 уровень, тогда как остальной штат

предприятия имеет допуск на уровни 1 и 2. Гостевые счета могут иметь допуск только уровня 1.

Для выполнения работ каждый процесс помечается допуском принципала, который работает с ним, он хранится в $C_{process}$. Кроме того, система помнит максимальный допуск для данных, которые процесс может видеть, $C_{maxseen}$. Система следует различным правилам для чтения и записи для того, чтобы санкционировать допуск и уберечь секретную информацию от раскрытия. Общее правило таково:

- перед чтением объекта, имеющего допуск C_{object}, проверяется $C_{object} <= C_{process}$;
- если предыдущее верно, то устанавливается $C_{maxseen} = \max(C_{maxseen}, C_{object})$ и выдаются права доступов.

Это правило может быть подытожено, как «нет чтения вверх». Процессу не разрешен доступ к информации более высокого класса, чем его допуск.

Соответствующее правило записи гласит: разрешить запись в объект с допуском C_{object} только, если $C_{maxseen} <= C_{object}$.

Это может быть названо, как «нет записи вниз». Все, что записано процессом, который читает данные с допуском C, должно иметь допуск C или выше. Понижение качества информации может быть сделано только после инспекции человеком. Почему? Программа не может принять решение по классификации: она может ошибочно записать все, что читает. Или, еще ху-же, программа может быть написана нарушителем! Например: редактор, чи-тающий конфиденциальные файлы.

Модель мандатного доступа предназначена для очень ответственной защиты, но компьютерные системы строятся на ее основе. У Федеральной Службы по техническому и экспортному контролю (ФСТЭК России) имеют-ся спецификации (Руководящие документы) на то, что должны обеспечивать такие системы (вслед за Оранжевой книгой, которая классифицирует систе-мы на основе их гарантий безопасности).

При разработке компьютерных систем, которые поддерживают модель контроля потока, следует доводить до предела предположения о слабостях в защите (например, о секретных каналах). Модель мандатного доступа часто снабжается отдельными сегментами и средствами по проверке целостности.

Для реализации модели монитора обращений в мандатной модели доступа необходимо создать программу, разграничивающую доступ к модели на

основе логических имен и паролей со списком управления доступом, осно-ванном на допусках (например, общий, внутренний и конфиденциальный). Создать не менее трех принципалов, имеющих права над данными объекта-ми:

- Принципал А имеет допуск уровня 3, то есть может читать любые предлагаемые объекты.
- Принципал В имеет допуск уровня 2, то есть может читать любые предлагаемые объекты за исключением конфиденциальных.
- Принципал С имеет допуск уровня 1 и может читать только общую информацию.

Примечание:

- В начале сеанса право на запись определяется: для А – только в объекты не ниже конфиденциальных, для В – в объекты не ниже для внутреннего ис-пользования, для С – в общедоступные объекты.
- В дальнейшем право на запись в объекты зависит от максимальной секретности документа, прочитанного в сеансе (* - свойство).

Программа должна разрешать доступ или отказывать в доступе любому числу пользователей с любой последовательностью запросов на чтение/запись. Дополнительным заданием может служить создание программы, которая отображает список субъектов и объектов с их допусками и метками для принципала – администратора безопасности.

Содержание отчета

1. Описание атаки НСД к информации в мандатной модели доступа при наличии пары: нарушитель – высокоуровневый сообщник.
2. Алгоритм, функциональная схема и функциональный состав программы.
3. Вывод, в котором предлагаются методы решения проблемы раскрытия (нарушения конфиденциальности) в мандатной модели доступа.

Контрольные вопросы

1. Перечислите источники угроз безопасности информационного общества.
2. В чем заключается угроза раскрытия информации? Какие еще угрозы Вы знаете?
3. Что положено в основу мандатной модели доступа?

4. Раскройте понятие «деклассификация» в контексте защиты информации в вычислительной системе.
5. Какова роль принципалов и объектов в операционной системе?
6. Какие средства позволяют реализовать мандатную модель доступа в ОС Novell Netware 4.12 (Windows 2000, XP)?
7. Какие средства позволяют реализовать Z-модель в ММД в ОС Novell Netware 4.12 (Windows 2000, XP)?
8. Расскажите о методах противодействия данной атаке.
9. Какие недостатки присущи мандатной модели помимо проблемы Z-системы?

ЛАБОРАТОРНАЯ РАБОТА № 4

Тема: Анализ информационной инфраструктуры государства.

Цель работы

Изучение процессов идентификации и аутентификации в вычислительной системе посредством создания собственной программы обработки пользовательского запроса на вход в систему. Реализация атаки на процесс идентификации/аутентификации пользователя в ОС Novell Netware 4.12 с целью определения пароля на вход в систему, а также изучение основных методов противодействия подбору пароля.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности» на темы «Анализ информационной инфраструктуры государства» и «Идентификация и аутентификация пользователя в вычислительной системе».
2. Изучить теоретический материал по курсу «Программирование» на тему «Вызов функций операционной системы» и «Ввод данных с клавиатуры».
3. Создать объект атаки утилитой SYSCON ОС Novell Netware 4.12.
4. Написать на языке Си программу ложного запроса на идентификацию и аутентификацию.

5. Проанализировать проделанную работу и предложить свой метод противодействия реализованной атаке.
6. Результаты отразить в отчете.

Краткие теоретические сведения

Системы информационного обеспечения органов ГМУ и управления можно разделить на следующие виды:

– государственные информационные системы;

– муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

– иные информационные системы (например, негосударственные системы, используемые в интересах предоставления информационных услуг органам ГМУ).

Только формирование информационной инфраструктуры территорий ГМУ, создание эффективных информационных ресурсов и соответствующих аналитических служб (подразделений) позволит обеспечить органы ГМУ ка-чественной информацией.

Идентификация и аутентификация принадлежат к основным компонентам политики безопасности. Отсутствие или низкая надежность процедур идентификации и/или аутентификации не позволяет противостоять атакам неуполномоченных субъектов на информационные ресурсы органов ГМУ путем предотвращения их регистрации в системе и отказа в получении доступа к ее ресурсам. Надежность механизмов идентификации/аутентификации напрямую влияет на уровень безопасности всей системы в целом. При необходимости эти процедуры могут быть усилены совместным применением нескольких механизмов идентификации и аутентификации.

Обход механизма идентификации/аутентификации может привести к различным по своей тяжести последствиям в операционной системе. Степень тяжести зависит от уровня предоставляемых возможностей:

- самый простой уровень включает только аутентификацию пользователей и предназначен для простейших систем, типа систем контроля доступа в помещения, в которых кроме идентификации и аутентификации реализована только функция регистрации входа;
- на втором уровне предполагается наличие специальных атрибутов (при-знаков), идентифицирующих конкретного субъекта и позволяющих выпол-

нить его авторизацию (предоставить ему соответствующие права для работы в системе). Этот уровень наиболее широко используется в операционных системах, в которых существуют атрибуты, определяющие степень привиле-гированности субъектов и уровень конфиденциальности объектов:

- на следующем уровне данные возможности расширяются путем регла-ментации принципов обработки результатов аутентификации, а также требо-ваниями к хранению, защите и предоставлению информации о результатах идентификации и аутентификации пользователей. Этот уровень используется в системах с четко определенной политикой управления доступом;
- на четвертом уровне происходит дальнейшее расширение требований, за-ключающееся в предоставлении возможностей установки специальных меха-низмов идентификации и аутентификации и их назначения для индивидуаль-ного пользователя и/или группы пользователей;
- на последнем уровне реализуется нескольких независимых механизмов аутентификации пользователей.

Рассмотрим в общем виде процесс входа в систему (login) для всех версий Novell Netware

- рабочая станция создает выделенный канал с сервером, присоединяясь к нему под именем NOT_LOGGED_IN и получает право на чтение каталога SYS:LOGIN;
- она загружает из него программу LOGIN.EXE и выполняет ее;
- происходит процесс идентификации и аутентификации на сервере под настоящим именем (различный для разных версии ОС);
- после этого, если необходимо, включается подпись пакетов для дальнейшего общения рабочей станции и сервера.

Определим объект атаки. Им является любой пользователь, имеющий идентификационное имя для входа в систему, а также – пароль, необходимый системе для аутентификации пользователя. При входе в систему пользова-тель вводит идентификационное имя и подтверждает его паролем.

Атака состоит в том, что создается программа с интерфейсом, похожим на интерфейс программы LOGIN.EXE используемой версии операционной системы. Затем она встраивается в загрузчик таким образом, чтобы ее выполнение как раз предшествовало запуску LOGIN.EXE. Программа-эмулятор

запрашивает имя (идентификация) и пароль (аутентификация) объекта атаки, сохраняет их в специальном файле для дальнейшего исследования; зате

атакуемому объекту выдается стандартное сообщение о неправильном вводе пароля и запускается настоящая программа LOGIN.EXE. Так нарушителю становится известна пара значений (идентификационное имя и пароль пользователя), необходимых для входа в систему.

Существенно трудным в выполнении этапом является внедрение про-граммы ложной идентификации/аутентификации в программу загрузки опе-рационной системы. Эта задача не является необходимой и может выпол-няться при желании выполняющего работу.

Содержание отчета

1. Описание отличительных особенностей программы – эмулятора.
2. Алгоритм, функциональная схема, состав и интерфейс программы.
3. Вывод, в котором предлагаются пути определения отличия эмулятора от настоящей программы идентификации/аутентификации, а также меры кото-рые должны быть реализованы в операционной системе для предотвращения запуска таких программ – эмуляторов.

Контрольные вопросы

1. Раскройте структуру понятия «безопасность национальных интересов в информационной сфере».
2. В чем заключается угроза нарушения целостности информации? Какие еще угрозы Вы знаете?
3. Для чего предназначены идентификация и аутентификация в вычислительной системе?
4. Как классифицируются процессы идентификации/аутентификации?.
5. В чем заключается атака по ложному запросу идентификации/аутентификации?
6. Укажите возможные последствия раскрытия пароля неавторизованным пользователем.
7. Какие средства ОС Novell Netware 4.12 (Windows 2000, XP) и языка Си позволяют реализовать эмулятор запроса на вход в систему?
8. Каким образом внедрить программу – эмулятор в процесс загрузки опе-рационной системы Novell Netware 4.12 пользователю, не обладающему пра-вом записи в файл загрузки и не имеющим права на изменение программы LOGIN.EXE?

ЛАБОРАТОРНАЯ РАБОТА № 5

Тема: Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации.

Цель работы

Изучение алгоритмов вызова программ в ОС MS DOS, а также принципов действия атак переполнения буфера ("buffer-overflow"). Применение основ информационной безопасности для нахождения путей противодействия угрозе. Реализация на практике модели атаки переполнения буфера в ОС MS DOS.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Изучить теоретический материал по курсу «Программирование» на тему «Передача параметров в программу средствами языка Си++», «Запуск про-грамм-потомков».
3. Написать на языке Си четыре программы:
   - программу, подверженную атаке переполнения буфера;
   - программу, защищенную от атак данного типа;
   - программу, реализующую атаку переполнения буфера;
   - программу типа EXPLOIT.
4. Проанализировать проделанную работу и предложить свой метод использования модификации адреса возврата.
5. Результат отразить в отчете.

Краткие теоретические сведения

Данная лабораторная работа посвящена исследованию атак типа переполнения буфера. Рассматривается одна из тех технологий, которая сегодня используется все чаще и требует для борьбы с ней понимания работы систе-мы.

Известно, что в результате некорректного обращения к памяти может возникнуть проблема с менеджером памяти или зависание. Как правило, это

связано с тем, что программа попыталась получить доступ к не принадлежащей ей области памяти. Это довольно часто случается, если программист забыл, например, проверить размеры строки, заносимой в буфер, и остаток строки попал в какие-то другие данные или даже в код. Это происходит из-за отсутствия контроля за размерами строк и буферов. Логичным следствием является наличие так называемых "buffer-overflow"-программ, которые в за-щищенных операционных системах используются для нарушения защиты системы и получения привилегий суперпользователя системы (в данной ла-бораторной работе в качестве модели используется ОС MS DOS).

Рассмотрим две программы, которые подвергаются атакам "buffer-overflow". Их отличие состоит в том, что одна из них подвержена атаке, а другая – нет. Обе программы имеют статически определенный буфер конеч-ного размера и принимают в качестве параметра строку неизвестной длины, которая заносится в этот буфер, признаком конца строки является нулевой символ. Во второй программе присутствует проверка на допустимую длину строки, в первой нет.

Для демонстрации работы этих двух программ необходимо написать специальную "buffer-overflow"-программу, которая вызывает программу-цель в режиме «с возвратом в предок» с параметром-строкой произвольного раз-мера.

Рассмотрим изменение состояния стека в процессе вызова программы-цели. Итак, стек (будем считать, что он растет вверх) перед вызовом функции main() программы-цели выглядит следующим образом (см. рис. 1).

	(область младших адресов)
	← Указатель вершины стека
	Использованная часть стека
	(область старших адресов)

Рис. 1. Состояние стека в процессе вызова программы (шаг 1).

Компилятор, встречая инструкцию вызова функции main(), заносит в стек смещение следующей после вызова команды. Таким образом, функция

main() завершив свою работу, будет знать адрес возврата управления. В результате стек имеет следующий вид (см. рис. 2).

	(область младших адресов)
	← Указатель вершины стека
RETADR	**← Адрес возврата**
PARAMS	**← Параметры функции**
	Использованная часть стека
	(область старших адресов)

Рис. 2. Состояние стека в процессе вызова программы (шаг 2).

Функции надо запомнить указатель на текущую верхушку стека BP, который будет использоваться в ссылке на параметры. Поэтому, независимо от архитектуры, выполняются следующие две инструкции,

```
push bp
mov bp, sp
```

Теперь в верхушке стека лежит предыдущее значение регистра BP, а сам он указывает на верхушку стека и может быть использован в качестве базового регистра при ссылке на параметры. В программах объявлен размер буфера в SIZE байт – этот буфер будет зарезервирован в стеке. После всех этих операций стек имеет следующий вид (см. рис. 3).

После всего этого программа работает прекрасно, пока дело не доходит до вызова функции strcpy(). Если длина строки меньше или равна длине буфера, то все пройдет хорошо, функция отработает, освободит зарезервированное пространство, восстановит регистр BP и вернет управление программе, которая очистит стек от переданных параметров. Если же длина строки будет больше размера буфера, то поскольку strcpy() копирует все символы, пока не встретит код конца строки – 0, часть строки затрет верхнюю часть стека и может испортить поле **RETADR**. Это станет заметно не сразу – все будет работать корректно, пока дело не дойдет до вызова return. Управление будет передано по адресу, который хранится в поле **RETADR**, но поскольку адрес испорчен, программа будет продолжать выполняться в некоторой точке адресного пространства, отличающейся от точки вызова. В этом месте воз-

никнет исключительная ситуация, и программа будет аварийно прервана, по-скольку маловероятно, чтобы адрес возврата указывал на какой-то осмыс-ленный код, причем находящийся в области памяти данной программы.

	(область младших адресов)
	← Указатель вершины стека
?????	**← Начало зарезервированного буфера**
?????	
?????	**← Конец буфера**
OLDBP	**← Старое значение регистра BP**
RETADR	**← Адрес возврата**
PARAMS	**← Параметры функции**
	Использованная часть стека
	(область старших адресов)

Рис. 3. Состояние стека в процессе вызова программы (шаг 3).

Избежать подобной ситуации можно по крайней мере двумя способами. Первый способ - контроль длины строки, копируемой в буфер. Этот способ необходимо реализовать в программе под номером 2.

Второй способ несколько необычен, но именно он помогает понять действие "buffer-overflow"-программ. Назовем программу, реализующую этот метод **OVERFLOW**. он состоит в следующем:

− файл-цель исследуется с помощью отладчика, например “Turbo Debugger”. Необходимо узнать **BP** и **RETADR**;

− программа OVERFLOW.EXE вызывает программу-цель с параметром – строкой, которая «затирает» поля **BP** и **RETADR** старыми, заранее извест-ными значениями этих полей. Параметром программы OVERFLOW.EXE яв-ляется имя файла, содержащего имя программы-цели (это поле должно зани-мать 13 символов), **BP** и **RETADR** (значения должны быть записаны в HEX -формате).

На практике для исследования программы-цели применяются так назы-ваемые **EXPLOIT**-программы. Их целью является осуществление атаки для формальной проверки исследуемой программы на устойчивость. **EXPLOIT**-программа запускает программу-цель со строкой переменной длины до тех пор, пока программа – цель не зависнет или не сообщит об ошибке. Если программа зависла, это означает, что в ней отсутствует проверка на длину входной строки. Следовательно, данная программа не защищена от атаки пе-реполнения буфера.

Программа должна запускаться с двумя параметрами:

- имя программы-цели;
- предельная длина строки.

В результате работы программы на экран дисплея должно выводится сообщение о текущем размере строки, передаваемой в качестве параметра программе-цели. Если весь вывод перенаправить в файл, то в случае успеш-ной атаки, то есть зависания системы, в этом файле можно будет узнать раз-мер последней строки. Таким образом, можно узнать размер буфера про-граммы-цели.

Содержание отчета

1. Описание атаки.
2. Алгоритм, функциональная схема и функциональный состав каждой программы.
3. Вывод должен содержать описание задач, для реализации которых применяются атаки переполнения буфера.

Контрольные вопросы

1. Каковы основные направления обеспечения информационной безопасности объектов информационной сферы государства?
2. Дайте классификацию методов нарушения конфиденциальности, целостности и доступности информации.
3. В чем заключается атака переполнения буфера?
4. Каковы могут быть последствия атаки в различных операционных системах?
5. Какие алгоритмы противодействия атаке переполнения буфера Вам известны?

6. Какие ошибки в программном обеспечении используются **EXPLOIT**-программами?
7. Можно ли использовать данную атаку для анализа программного обеспечения?

ЛАБОРАТОРНАЯ РАБОТА № 6

Тема: Причины, виды, каналы утечки и искажения информации.

Цель работы

Изучение основных задач, моделирование и реализация на практике процесса регистрации и учета событий в ОС MS-DOS с целью практического применения основ защиты информации, а также для ознакомления с системой прерываний данной операционной системы. Ознакомление с основными методами обработки результатов аудита Осуществление на практике одного из методов обработки аудита клавиатуры с целью более полного представления об алгоритмах работы программ типа «Intrusion Detection».

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности» на тему «Регистрация и учет событий в вычислительной сис-теме» и «Обработка результатов аудита».
2. Изучить теоретический материал по курсу «Программирование» на тему «Создание резидентных программ», «Работа с файлами», «Ввод данных с клавиатуры» и «Алгоритмы сортировки».
3. Написать на языке Си программу, реализующую протоколирование всех нажатий клавиш в файле аудита клавиатуры, а также времени их нажатия Исключение составляют триггерные клавиши, для них необходимо фиксиро-вать только те нажатия, которые влияют на смену их состояния Программа должна позволять выполнять любые операции операционной системы и не должна мешать работе других программ, то есть она должна работать в так называемом фоновом режиме. Файл аудита клавиатуры должен иметь имя, длиной не более восьми символов, которое должно быть уникальными для каждого пользователя. Необходимо реализовать предотвращение повторного

запуска программы-аудита и отгрузку ее из памяти, то есть управление резидентной частью. Пользователь, выполняющий роль администратора аудита, должен иметь следующие возможности в части запуска и отключения аудита: – временное отключение аудита;

– определение информации о состоянии аудита (установлен или нет);

– задание идентификационного имени пользователя, для которого необходимо запускать аудит (не должно превышать восьми символов);

– располагать файлы аудита удобным для администратора образом, т.е. файл аудита не должен быть жестко привязан ни к какому конкретному ката-логу или диску.

4. Написать на языке Си программу обработки данных аудита клавиатуры, анализирующую содержимое командной строки ОС MS-DOS (или время ра-боты в ОС).

5. Проанализировать проделанную работу с целью нахождения путей при-менения аудита клавиатуры. В качестве альтернативы можно придумать и реализовать свою программу обработки результатов аудита клавиатуры.

6. Результаты отразить в отчете.

Краткие теоретические сведения

Мощность современных сетей и причина, по которой они используются, заключаются в способности к быстрой передаче информации. Эта возможность передачи информации представляет также проблему безопасности. Сетевая информация, полученная из базы данных или посланная по электронной почте, может легко выйти из-под контроля. Она может ошибочно оказаться в почтовом ящике другого лица, или может быть собрана из кажущихся безобидными битов данных в критически опасные информационные обзоры, раскрывающие производственные планы, стратегии рынка или бизнес-планы. Поэтому важно контролировать возможности распространения и утечки информации. Для этих целей применяется аудит.

Аудит – это регистрация и учет событий, осуществляемых пользователем в системе. События в данном случае представляют собой нажатия на клавиши. Таким образом, происходит фиксирование информации, введенной пользователем с клавиатуры.

Так как MS-DOS является однозадачной операционной системой, то в определенный момент времени в ней может работать только один пользова-

тель, поэтому в программе аудита должен присутствовать механизм иденти-фикации, позволяющий для каждого пользователя определить идентифика-ционное имя, которое используется для наименования файла аудита. Файл аудита содержит информацию о действиях пользователя в системе:

- время входа с систему (время запуска программы-аудита);
- специальная информация, которая зависит от назначения аудита.

Специальная информация определяется целью аудита. Цель аудита – фиксирование попыток со стороны пользователя осуществить неавторизо-ванные, то есть недозволенные, действия, а также те действия, которые могут повлечь за собой нарушение работоспособности системы Примеры неавтори-зованных действий:

- работа за терминалом в недозволенное время. Определяется с помощью аудита клавиатуры путем анализа времени протоколирования нажатия на клавишу;
- запуск программ. приводящий к нарушению работоспособности операци-онной системы. Определяется с помощью аудита клавиатуры, если команда на запуск программы поступает из командной строки, а не с помощью другой программы.

Административные ограничения могут накладываться также на функции создания, удаления, переименование файлов и каталогов. Такие контролирующие действия вынуждают пользователя быть дисциплинированным. Таким образом, аудит – средство, позволяющее проверять выполнение требований, предъявляемых пользователю администратором системы, отвечающим за нормальное функционирование операционной системы и целостность хранящихся в ней данных.

Выполнение программы в фоновом режиме возможно, благодаря возможности создания резидентных программ. Отличительное свойство резидентных программ (TSR – Terminate-but-Stay-Resident) состоит в том, что они после своего завершения остаются в памяти компьютера, а операционная система помечает занятую ими память как используемую. Использование TSR позволяет реализовать так называемое пассивное мультипрограммирование MS-DOS является однопрограммной операционной системой, но активизация TSR вызывает переключение компьютера на резидентную программу. Если активизация TSR выполняется периодически, появляется возмож-ность выполнения программ на фоне других программ.

Следующее обязательное требование к надежно работающей TSR – предотвращение повторного вхождения в MS-DOS. Однопрограммная MS-DOS не является реентерабельной. Реентерабельная программа – это программа, которая разрешает в силу особенностей своего построения, начинать ее выполнение несколько раз, не дожидаясь завершения выполнения (выхо-да) программы, начатого ранее. Реентерабельная программа не изменяет ни одной константы или переменной, которые могут повлиять на повторное вы-полнение программы. Большинство программ, образующих в совокупности ядро MS-DOS, не являются реентерабельными. В этой связи не являются ре-ентерабельными и программы, обращающиеся к функциям MS-DOS непо-средственно, либо через функции библиотеки языка Си. Для TSR, написан-ной на языке Си, всегда существует вероятность повторного вхождения в MS-DOS, так как TSR может получить управление в любой момент, в том числе и тогда, когда MS-DOS выполняет нереентерабельную секцию своего кода. Отсюда следует требование к ISR активизировать TSR только тогда, когда MS-DOS позволяет повторное вхождение.

Кроме опасности повторного вхождения в MS-DOS необходимо предотвращать повторное вхождение в TSR до ее завершения (то есть если TSR может прерваться запуском самой себя), переключение стека на один и тот же массив неизбежно приведет к ошибке. При повторном вхождении в стеке будут затерты данные, относящиеся к первому, еще не завершенному вхож-дению.

В зависимости от системы аудита применяют тот или иной метод обработки данных. Рассмотрим два метода обработки данных аудита клавиатуры:

- анализатор командной строки ОС MS-DOS. Цель – выделить из потока данных о нажатых клавишах информацию, введенную пользователем в командной строке и автоматически проанализировать наличие несанкционированных действий (например, запуск программы TETRIS.EXE) Результатом работы программы обработки является создание списка пользователей, совершающих несанкционированные действия, ранжированного по степени тяжести нарушения, которая определяется администратором аудита;
- контроль времени работы в системе. Цель – произвести анализ потока данных аудита клавиатуры применительно ко времени нажатия клавиш, ин-формирующих о работе пользователя в системе. Результатом

работы про-граммы является создание списка пользователей, работающих во внеурочное

для них время, и определение штрафных санкций, предусмотренных администратором.

Содержание отчета

1. Описание назначения аудита клавиатуры.
2. Объяснение механизма прерываний в ОС MS-DOS.
3. Алгоритм функционирования программы в фоновом режиме.
4. Алгоритм предотвращения повторного запуска, отгрузки программы.
5. Алгоритм обхода нереентерабельности в ОС MS-DOS.
6. Алгоритм записи информации в файл аудита.
7. Описание реализованного метода обработки аудита клавиатуры.
8. В выводе необходимо представить недостатки данного подхода к созданию системы аудита в операционной системе и пути их решения. Вывод должен содержать мотивацию выбора реализованного метода

Контрольные вопросы

1. Перечислите источники угроз безопасности информационного общества.
2. В чем заключается угроза распространения и утечки информации? Какие еще угрозы Вы знаете?
3. Объясните понятие аудита в контексте безопасности вычислительных систем.
4. С помощью какого механизма ОС MS-DOS поддерживает одновременную работу нескольких программ?
5. Как реализовать перехват прерывания средствами языка Си?
6. В чем заключается задача аудита клавиатуры?
7. Как реализовать аудит клавиатуры в ОС MS-DOS?
8. Какие проблемы возникают при записи информации в файл аудита?
9. Что такое реентерабельность?
10. Какие способы обхода повторного вхождения в MS-DOS и в обработчик прерывания Вы знаете?
11. Как реализовать управление резидентной частью программы?
12. Для чего необходима идентификация в системе аудита?
13. Перечислите недостатки данного подхода к реализации аудита для защиты операционной системы.
14. Предложите пути устранения этих недостатков.

15. Для чего необходима аутентификация пользователя?
16. Существует ли возможность отключения аудита помимо предусмотренной?
17. Приведите примеры несанкционированных действий пользователя в ОС MS-DOS.
18. Для чего предназначены программы обработки данных аудита?
19. Что Вы понимаете под проникновением в систему защиты?
20. Какие методы обработки данных аудита клавиатуры Вы знаете?
21. В чем заключается метод анализа командной строки в ОС MS-DOS?
22. В чем заключается анализ времени работы в операционной системе?
23. В чем заключается Ваш метод обработки данных аудита клавиатуры?

ЛАБОРАТОРНАЯ РАБОТА № 7

Тема: Технические средства и методы защиты информации.

Цель работы

Разработать комплекс мероприятий по защите информации от возможной утечки информации за счет постоянных электромагнитных излучений (ПЭМИ) и наводок, основанных на использовании система активной защиты (САЗ) ВОЛНА-3М указанной зоны.

Подготовка и порядок выполнения работы

1. Определить зону размещения основных технических средств (ОТС) ЭВТ (видеотерминальные устройства, ПЭВМ, периферийные пункты и другие вы-числительные комплексы, входящие в состав рассредоточенных систем об-работки информации).
2. Произвести подбор варианта размещения системы активной защиты ВОЛНА-3М (рис. 6, 7, 9, 10, 11).
3. Произвести размещение и подключение САЗ ВОЛНА-3М.
4. Произвести контроль работы САЗ ВОЛНА-3М путем включения бытового приемника.
5. Подготовить отчет в соответствии с пунктами 1-4.

Краткие теоретические сведения

Описание применения

Система активной защиты ВОЛНА-3М предназначена для защиты видеотерминальных устройств, ПЭВМ, периферийных пунктов и других вы-числительных комплексов, которые могут входить в состав рассредоточен-ных систем обработки информации от возможной утечки информации за счет постоянных электромагнитных излучений (ПЭМИ) и наводок; применяется на объектах ЭВТ I, II и III-ей категорий и обеспечивает их защиту в случаях недостаточной контролируемой зоны (КЗ) или если границей КЗ являются стены здания объекта.

САЗ применяется в тех случаях, когда для основных технических средств и систем (ОТСС) ЭВТ невозможно обеспечить требуемые размеры контролируемой зоны, приведенные в предписаниях по эксплуатации, или системы электропитания и заземления ОТСС ЭВТ не соответствуют требова-ниям указанного документа, а также, если невозможно обеспечить требуемое удаление от ОТСС ЭВТ вспомогательных технических средств и систем (ВТСС), имеющих выход за пределы КЗ.

Диапазон шумовых сигналов САЗ ВОЛНА-3М от 0,5 до 1000 МГц, что обеспечивает возможность маскирования ПЭМИ от терминальных устройств (дисплеев), накопителей на магнитных дисках и других ОТСС ЭВМ, имею-щих информативные побочные излучения в указанном диапазоне частот.

САЗ включает в себя генератор шумовых сигналов со встроенной схемой автоконтроля и антенную систему. Устройство выполнено в виде настенного блока, габаритные и установочные размеры приведены на рис. 4.

Нагрузкой шумовых каналов САЗ ВОЛНА-3М служат 4 контура рамочных антенн. Эти контуры образуются проволочными рамками, разме-щенными на стенах, полу и потолке помещения. Схема внешних соединений приведена на рис. 5.

Электропитание САЗ осуществляется от сети переменного тока частотой 50 Гц, напряжением 220 В. Включение производится тумблером «сеть», расположенным на его нижней панели. После включения на передней панели должен засветиться светодиод красного цвета. При неисправности САЗ (вы-

ходе из стоя генератора или обрыве проводов антенн) светодиод гаснет и одновременно замыкаются контакты 5, 6 разъема X2.

Клемма блока генераторов X8 «⊥» должна быть соединена с контуром заземления.

Потребляемая мощность устройства – не более 15 Вт.

Уровни шумового поля, создаваемого САЗ, соответствуют требованиям ГОСТ 23450-79 («Радиопомехи индустриальные от промышленных, научных и медицинских высокочастотных установок») и медико-биологическим нормам (ГОСТ 12.1.006-84) при круглосуточном пребывании персонала на рабочих местах, размещенных не ближе 1,0 м от устройств САЗ и проводов рамочных антенн.

Эффективность маскирующего действия САЗ определяется аппаратурными измерениями в соответствии с методиками Гостехкомиссии РФ методиками контроля объектов ЭВТ. Периодическая проверка работоспособности проводится по методике, представленной в Приложении А.

Защита информации от утечки за счет побочных электромагнитных излучений ОТСС ЭВТ

При использовании для маскирования ПЭМИ, САЗ размещается на стене ближайшей к контролируемой зоне (возможно на полу или потолке), между защищаемыми ОТСС и точками возможного перехвата. Типовые варианты размещения рамочных антенн одного комплекта САЗ ВОЛНА-3М приведены на рис. 6, 7. На рис. 8 показана схема размещения двух комплектов САЗ ВОЛНА-3М. Если защищаемое ОТС ЭВТ расположено на втором этаже или выше, причем одна из стен помещения, где размещено ОТС, выходит на неконтролируемую территорию (здание с «нулевой» КЗ), то рамочные антенны располагаются в двух плоскостях как показано на рис. 9.

Как правило антенные рамки должны располагаться симметрично относительно основного блока САЗ: две рамки вправо от него, две – влево. Плоскости рамок могут изгибаться (см. рис. 10).

Площадь большой рамочной антенны должна находиться в пределах от 2 $м^2$ до 8 $м^2$, а малой – от 0,5 $м^2$ до 1,5 $м^2$, при этом рамочные антенны должны размещаться на таком удалении от основного блока САЗ, чтобы длина провода рамочной антенны не превышала 13 м. Рамочный антенны выполняются механически прочным многожильным изолированным проводом се-чением не менее 0,35 $мм^2$. Активное сопротивление каждой рамочной антен-ны должно быть не более 2,0 Ом.

Для устойчивой работы САЗ рекомендуется рамочные антенны выполнять проводом с активным сопротивлением не более 1,0-1,5 Ом. Если сопротивление антенны оказывается выше требуемого, рекомендуется применить провод большего сечения.

Допускается использовать САЗ для защиты ОТСС ЭВТ, установленных в помещениях с декоративной отделкой металлическими панелями. В этом случае металлические панели используются в качестве части контура рамочной антенны (рис. 11).

Защита информации от утечки за счет наводок на линии электропитания и заземления ОТСС ЭВТ

Система активной защиты ВОЛНА-3М можно использовать для маски-рования наведенных сигналов от ОТСС ЭВТ в сети электропитания или шине заземления.

Для защиты сети электропитания САЗ должна запитываться непосредственно от сети электропитания ОТСС ЭВТ, от розетки, ближайшей к рас-пределительному щитку, в ближайшей точке выхода линии сети электропи-тания из помещения, в котором установлены ОТС ЭВТ, а одна из рамочных антенн должна быть соединена с заземляющим проводом трехпроводной се-ти электропитания (см. рис. 12).

Для зашумления цепи заземления необходимо подключить САЗ к цепи заземления на границе КЗ или в ближайшей к ней удобной точке (например, в месте выхода шины заземления из помещения, в котором размещены за-щищаемые ОТСС ЭВТ).

Маскирующий шум подается в шину заземления посредством подключения к ней одной из рамочных антенн, как это показано на рис. 13. Место соединения САЗ с заземляющим проводом сети электропитания или шиной заземления выбирается так, чтобы шумовой сигнал подавался в точку, расположенную ближе к границе КЗ, чем защищаемое ОТС ЭВТ, причем потенциальный выход (разъем X2) подключается в направлении к границе КЗ, а заземляющий выход (разъем X6) в направлении ОТСС ЭВТ.

Длина участка шины заземления или заземляющего провода сети электропитания (а), включенного в контур рамочной антенны САЗ, должна быть в пределах 1-2 м, общая длина с учетом подводящих проводов не должна превышать 8 м.

Защита информации от утечки за счет наводок на линии ВТСС, выходящие за пределы КЗ

Если на объекте ЭВТ имеются вспомогательные технические средства и системы (ВТСС), линии которых имеют выход за пределы КЗ, и их удаление от ОТСС ЭВТ меньше требуемых значений, для маскирования наведенных на линии ВТСС информативных сигналов могут использоваться САЗ.

В этом случае антенны САЗ необходимо прокладывать в непосредственной близости от линий ВТСС, обеспечив пробег не менее 2 м для неэкра-нированных линий ВТСС, либо использовать экранирующую оболочку кабе-ля ВТСС в качестве части контура рамочной антенны.

При большом количестве ВТСС САЗ рекомендуется размещать в местах, где произведена кроссировка линий ВТСС, подлежащих защите, например, АТС, распределительных шкафах и т.п. (рис. 14).

Три рамочных антенны САЗ ВОЛНА-3М прокладываются в непосредственной близости от кабелей ВТСС, например, по кабель-ростам кроссов АТС, по периметру (с внутренней стороны) распределительных шкафов и коробок, а четвертая антенна подключается к заземленным корпусам указан-ного оборудования.

Содержание отчета

Отчет должен содержать:

1. схему размещения ОТС ЭВТ;
2. схему определение границ контролируемой зоны;
3. схему выбранного варианта размещения САЗ ВОЛНА-3М;
4. описание размещения и подключения САЗ ВОЛНА-3М;
5. описание результатов контроля САЗ путем подключения бытового радиоприемника.

Контрольные вопросы

1. Определите диапазон шумовых сигналов САЗ ВОЛНА-3М.
2. Определите максимальное значение активного сопротивления каждой рамочной антенны САЗ ВОЛНА-3М.
3. Определите максимальное значение длины провода МГШВ рамочной антенны САЗ ВОЛНА-3М.
4. Что служит нагрузкой шумовых каналов САЗ ВОЛНА-3М?

5. Какова частота переменного тока, с которой осуществляется электропитание в сети для САЗ ВОЛНА-3М?
6. Каково напряжение, при котором осуществляется электропитание САЗ ВОЛНА-3М?
7. Каково активное сопротивление каждой рамочной антенны для САЗ ВОЛНА-3М?

Рис. 4. Габаритные и установочные размеры устройства ВОЛНА-3М.

Рис. 5. Схема внешних соединений устройства ВОЛНА-3М.

Рис. 6. Вариант размещения САЗ ВОЛНА-3М (I).

Рис. 7. Вариант размещения САЗ ВОЛНА-3М в помещении малой площади.

Рис. 8. Размеры рамочных антенн САЗ и их взаимное размещение.

Рис. 9. Вариант размещения САЗ ВОЛНА-3М с горизонтальными антеннами.

Рис. 10. Вариант размещения САЗ ВОЛНА-3М

Рис. 11. Размещение САЗ в помещениях с декоративной отделкой металлическими панелями.

Рис. 12. Схема подключения САЗ к сети электропитания.
1 – ОТС ЭВТ; 2 – САЗ; 3 – цепь электропитания ОТС ЭВТ; 4 – шина заземления; 5 – антенная система САЗ; 6 – стены помещения, где размещено ОТС ЭВТ; а – плечо нагрузки.

Рис. 13. Схема подключения САЗ к шине заземления.
1 – ОТС ЭВТ; 2 – САЗ; 3 – сеть электропитания; 4 – шина заземления (заземляющий провод 3-х проводной сети); 5 – антенная система САЗ; 6 – стены помещения, где размещено ОТС ЭВТ; а – участок шины заземления (плечо нагрузки).

Рис. 14. Схема подключения САЗ к ВТС.
1 – САЗ; 2 –сеть электропитания; 3 – шина заземления; 4 – корпус кросса; 5 – антенная система САЗ.

ЛАБОРАТОРНАЯ РАБОТА № 8

Тема: Программно-аппаратные средства обеспечения информационной безопасности.

Цель работы

Получение навыков по практическому применению Программно-аппаратного комплекса средств защиты информации (ПАК СЗИ) от несанк-ционированного доступа (НСД) «Аккорд-АМДЗ (аппаратный модуль дове-ренной загрузки)».

Подготовка и порядок выполнения работы

1. Изучить теоретический материал по разделу ПАК СЗИ «Аккорд».
2. Построить систему защиты информации на основе ПАК СЗИ от НСД «Аккорд» (планирование применения комплекса).
3. Установить в ПЭВМ аппаратную часть комплекса: плату контроллера и контактное устройство (съемник информации) и произвести регистрацию администратора безопасности информации (administrator).
4. Настроить контроллер комплекса с учетом конфигурации технических и программных средств ПЭВМ, а также установить на жестком диске ПЭВМ программное обеспечение комплекса с дистрибутивных дискет.
5. Настроить дистрибутивные средства комплекса в соответствии с правилами разграничения доступа к информации.
6. Произвести работу с журналами регистрации.
7. Произвести снятие ПАК СЗИ от НСД «Аккорд» с ПЭВМ.
8. Результаты проделанной работы отразить в отчете.

Краткие теоретические сведения

Описание применения

Перед установкой и эксплуатацией комплексов СЗИ НСД «Аккорд-АМДЗ» необходимо внимательно ознакомиться с представленными материалами, в которых отражена эксплуатационная документация на комплекс, а также принять необходимые защитные организационные меры.

Применение защитных средств комплексов должно дополняться общими мерами технической безопасности.

Основные принципы организации защиты информации от НСД и обеспечения ее конфиденциальности

Мероприятия по защите информации от НСД являются составной частью управленческой, научной, производственной (коммерческой) деятельности предприятия (учреждения, фирмы и т.д.), независимо от их ведомственной принадлежности и формы собственности, и осуществляются в комплексе с другими мерами по обеспечению установленного режима конфиденциальности.

Практика организации защиты информации от НСД при ее обработке и хранении в (автоматизированной системе) АС должна учитывать следующие принципы и правила обеспечения безопасности информации:

1. Соответствие уровня безопасности информации законодательным поло-жениям и нормативным требованиям по охране сведений, подлежащих защи-те по действующему законодательству, в том числе выбор класса защищен-ности АС в соответствии с особенностями обработки информации (техноло-гия обработки, конкретные условия эксплуатации АС) и уровнем ее конфи-денциальности.
2. Выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите, его своевременная кор-ректировка.
3. Наиболее важные решения по защите информации должны приниматься руководством предприятия (организации, фирмы), владельцем АС.
4. Определение порядка установления уровня полномочий субъектов доступа, а также круга лиц, которым это право предоставлено.
5. Установление и оформление правил разграничения доступа (ПРД), то есть совокупности правил, регламентирующих права доступа субъектов доступа к объектам доступа.
6. Установление личной ответственности пользователей за поддержание уровня защищенности АС при обработке сведений, подлежащих защите по действующему законодательству путем:

- ознакомления с перечнем защищаемых сведений, организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
- определения уровня полномочий в соответствии с его должностным предназначением;

− получения от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации.

7. Обеспечение физической охраны объекта, на котором расположена защи-щаемая АС (территория, здания, помещения, хранилища информационных носителей), путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи.

8. Организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информацион-ных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информа-ции и т.д.

9. Планомерный и оперативный контроль уровня безопасности защищаемой информации согласно нормативным документам (НД) по безопасности ин-формации, в том числе проверка защитных функций средств защиты инфор-мации.

10.Средства обработки и защиты информации должны иметь СЕРТИФИКАТ, удостоверяющий их соответствие требованиям по безопасности информации.

Назначение комплекса СЗИ НСД «Аккорд-АМДЗ»

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа – аппаратный модуль доверенной загрузки «Аккорд-АМДЗ» предназначен для применения на ПЭВМ (PC) типа IBM PC для защиты ПЭВМ (АС) и информационных ресурсов от НСД и контроля це-лостности файлов и областей HDD (в том числе и системных) при много-пользовательском режиме их эксплуатации. При этом обеспечивается режим доверенной загрузки в различных операционных средах: MS DOS, Windows 3.x, Windows 95/98, Windows NT, OS/2, UNIX.

Комплекс представляет собой совокупность технических и программных средств, предназначенных для выполнения основных функций защиты от НСД ПЭВМ (АС) на основе:

- применения персональных идентификаторов пользователей;

\

- парольного механизма;
- блокировки загрузки операционной системы со съемных носителей информации;
- контроля целостности технических средств и программных средств (файлов общего, прикладного программного обеспечения и данных) ПЭВМ (АС);
- обеспечения режима доверенной загрузки* установленных в ПЭВМ (АС) операционных систем, использующих любую из файловых систем: FAT 12, FAT 16, FAT 32, NTFS, HPFS, FreeBSD.

*Под термином «доверенная загрузка» понимается загрузка операционной системы только после проведения контрольных процедур идентификации/аутентификации пользователей, проверки целостности технических и программных средств ПЭВМ (РС) с использованием алгоритма пошагового контроля целостности.

Комплекс СЗИ НСД «Аккорд-АМДЗ» разработан ОКБ САПР при участии фирмы «ИнфоКрипт ЛТД» на основании лицензии Гостехкомиссии России и производится на аттестованном производстве.

Характеристика комплекса СЗИ НСД «Аккорд-АМДЗ»

Комплекс СЗИ НСД «Аккорд-АМДЗ» выпускаются в программно-аппаратном исполнении, и поставляется в различных модификациях.

Вся программная часть комплекса (включая средства администрирования), список пользователей и журнал регистрации размещены в энергонезависимой памяти контроллера. Этим обеспечивается возможность проведения идентификации или аутентификации пользователей, контроля целостности технических и программных средств ПЭВМ (РС), администрирования и аудита на аппаратном уровне, средствами контроллера комплекса до загрузки ОС.

Комплекс «Аккорд-АМДЗ» реализуется на основе контроллеров «Аккорд-4++», «Аккорд-4.5», «Аккорд-5» и их модификаций, приведенных в таблице 1.1.

Все модификации комплекса «Аккорд-АМДЗ»:

- могут использоваться на ПЭВМ с процессором 80266 и выше, объемом RAM 628 Кбайт при наличии свободного слота ISA (PSI) на материнской плате ПЭВМ;

– используют для идентификации пользователей уникальные персональные ТМ-идентификаторы DS 1992 – DS 1996 с объемом памяти до 64 Кбит и пре-дусматривают регистрацию до 32 пользователей на ПЭВМ (рабочей станции ЛВС);

– используют для аутентификации пользователей пароль до 12 символов, вводимый с клавиатуры;

– блокируют загрузку с отчуждаемых носителей (FDD, CD ROM, ZIP-drive);

– обеспечивают контроль целостности аппаратных средств ПЭВМ до загрузки ОС;

– обеспечивают контроль целостности программ и данных до загрузки ОС, защиту от внедрения разрушающих программных воздействий (РПВ);

– поддерживают файловые системы следующих типов; FAT12, FAT16, FAT32, NTFS, HPFS, FreeBSD;

– осуществляют регистрацию действий пользователей в системном журнале, размещенном в энергонезависимой памяти контроллера;

– обеспечивают администрирование системы (регистрацию пользователей и персональных идентификаторов, назначение файлов для контроля целостно-сти, контроль аппаратной части ПЭВМ, просмотр системного журнала);

– осуществляют разграничение прав доступа пользователей в соответствии с уровнем их полномочий (при установке специального ПО).

Дополнительно могут устанавливаться следующие блоки:

– аппаратный датчик случайных чисел для криптографического применения – опция К;

– блокировка до двух физических каналов (FDD, CD-ROM, ZIP-drive отчуждаемых носителей) – опция С;

– интерфейс RS-232 для подключения считывателя smart-карт;

– таймер реального времени с отдельным источником питания.

При модификации системного ПО замена контроллера не требуется.

При этом обеспечивается поддержка специального режима программирования контроллера без снижения уровня защиты.

Для обеспечения разграничения доступа пользователей совместно с комплексом может поставляться (по отдельному заказу) специальное ПО:

1. v.1.35 – при работе ПЭВМ (PC) под управлением ОС MS DOS, Windows 3.x;
2. v.1.95 – при работе ПЭВМ (PC) под управлением ОС Windows 95;

3. v.2.0 – при работе ПЭВМ (PC) под управлением ОС Windows NT 4.0+SP4;
4. v.2.3 – для использования штатных средств разграничения доступа ОС Windows NT совместно с комплексом «Аккорд-АМДЗ».

Таблица 1

Модификации комплекса СЗИ НСД «Аккорд-АМДЗ»

Особенности различных типов контроллеров	**«Аккорд-4++»**	**«Аккорд-4.5»**	**«Аккорд-5»**
Тип используемой системной шины	ISA	ISA	PCI
Установка реле управления физическими линиями (5 В, 300 мА)	Не предусмотрена	Возможна установка 2-х реле по заказу	Возможна установка 2-х реле по заказу
Возможность перепрограммирования всех элементов без изменения аппаратной части	+	+	+
Установка таймера реального времени с автономным источником питания	Не предусмотрена	Возможна установка по заказу	Возможна установка по заказу
Установка датчика случайных чисел для криптографических применений	Не предусмотрена	Производится для всех контроллеров данного типа	Производится для всех контроллеров данного типа

Поставляемое совместно с комплексом «Аккорд-АМДЗ» специальное ПО реализует возможности разграничения доступа и позволяет администратору безопасности информации (администратору БИ) описать правила разграничения доступа (ПРД) на основе наиболее полного набора атрибутов доступа:

1. При операциях с файлами:
   R – разрешение на открытие файлов только для чтения;
   W – разрешение на открытие файлов для записи;
   C – разрешение на создание файлов на диске;
   D – разрешение на удаление файлов;
   N – разрешение на переименование файлов и подкаталогов;

O – эмуляция разрешения на запись информации в файл, имеющий более низкий приоритет, чем атрибут W (разрешение на открытие файлов для записи).

V – видимость файлов. Позволяет делать существующие файлы невидимыми для программ. Атрибут V имеет более высокий приоритет, чем атрибуты R, W, D, N, O;

2. При операциях с каталогами:

M – разрешение на создание подкаталогов;

E – разрешение на удаление подкаталогов;

G – разрешение перехода в конкретный каталог (доступность каталога);

3. При операциях с программами (задачами):

X – разрешение на запуск программ;

4. Атрибуты принудительной регистрации:

r – всех операций чтения файла в журнале регистрации;

w – всех операций записи файла в журнале регистрации.

Такой набор атрибутов позволяет реализовать любую разумную непротиворечивую политику информационной безопасности, обеспечить конфи-денциальное делопроизводство.

Условия применения комплекса СЗИ НСД «Аккорд-АМДЗ»

Для установки комплекса «Аккорд-АМДЗ» требуется следующий минимальный состав технических и программных средств:

- IBM PC совместимая ПЭВМ, работающая под управлением операционной системы, поддерживающей любую из файловых систем FAT 12, FAT16, FAT 32, NTFS, HPFS, FreeBSD;
- наличие свободного слота (ISA/PCI) на материнской плате ПЭВМ;
- при поставке совместно с комплексом специального программного обес-печения – объем дискового пространства для его размещения на логическом диске C: для ПО v.1.35 – около 1,2 Мбайт, для ПО v.1.95 – около 2,0 Мбайт, для ПО v.2.0, 2.3 – около 1,5 Мбайт.

При модификации внутреннего программного обеспечения замена кон-троллера не требуется. При этом обеспечивается поддержка специального режима программирования контроллера без снижения уровня защиты.

Технические средства защищаемой ПЭВМ не должны содержать аппаратно-программных механизмов, ориентированных на целенаправленное нарушение правильности функционирования комплекса.

Для эффективного применения средств защиты комплекса и поддержания необходимого уровня защищенности ПЭВМ (АС) и информационных ресурсов требуется:

- физическая охрана ПЭВМ (АС) и ее средств, в том числе проведение мероприятий по недопущению изъятия контроллера комплекса;
- наличие администратора безопасности информации (БИ) – привилегиро-ванного пользователя, имеющего особый статус и абсолютные полномочия. Обязанности администратора БИ по применению комплекса изложены в «Руководстве администратора»;
- учет носителей информации и ТМ-идентификаторов пользователей;
- периодическое тестирование средств защиты комплекса «Аккорд»;
- использование в ПЭВМ (АС) технических и программных средств, сертифицированных как в Системе ГОСТ, так и в ГСЗИ.

Состав комплекса СЗИ НСД «Аккорд-АМДЗ»

Комплекс СЗИ НСД «Аккорд-АМДЗ» включает программные и аппаратные средства.

Аппаратные средства

Одноплатный контроллер представляет собой электронную плату, устанавливаемую в свободный слот материнской платы ПЭВМ (PC). Контроллер изготовлен по современной технологии многослойных печатных плат с покрытием химическим золотом с использованием наиболее современной элементной базы, является универсальным, не требует замены при переходе к другим типам операционных систем. В контроллере комплекса аппаратно реализована работа с каналом Touch Memory, что обеспечивает надежную работу с идентификаторами DS-199x на всех типах ПЭВМ (PC).

Контактное устройство – съемник информации с ТМ-идентификаторов пользователей (устройств памяти DS 199x «Touch memory»).

Персональные ТМ-идентификаторы пользователей представляют собой полупассивные микропроцессорные устройства DS 199x («Touch

memory»), снабженные элементом питания, в виде «таблетки» диаметром 16 мм и тол-

щиной 3-5 мм в удобной пластмассовой (металлической) оправке. Каждый ТМ-идентификатор обладает уникальным номером (48 бит), который форми-руется технологически и подделать который практически невозможно.

Объем доступной для записи/чтения памяти составляет до 64 Кбит в зависимости от типа идентификатора. Срок хранения записанной информа-ции, обеспечиваемый элементом питания не менее 10 лет.

Количество и тип ТМ-идентификаторов, модификация контроллера и контактного устройства оговаривается при поставке комплекса.

Программные средства, размещенные в энергонезависимой памяти компьютера (ЭНП) контроллера комплекса

В состав программных средств входят:

- BIOS контроллера комплекса «Аккорд-АМДЗ»;
- программное обеспечение АМДЗ, в составе следующих функциональных модулей:

1. средства идентификации пользователей;
2. средства аутентификации пользователей;
3. средства контроля целостности технических средств ПЭВМ (PC);
4. средства контроля целостности системных областей жесткого диска;
5. средства контроля целостности программных средств;
6. средства аудита (работа с журналом регистрации событий);
7. средства администрирования комплекса.

Специальное ПО СЗИ НСД

По отдельному заказу совместно с комплексом АМДЗ может поставляться следующее ПО разграничения доступом:

1. версия 1.35 – для MS DOS;
2. версия 1.95 – для Windows 95/98;
3. версия 2.0, 2.3 – для Windows NT.

Надежность функционирования системы защиты ПЭВМ (PC) от НСД обеспечивается выполнением средствами СЗИ НСД «Аккорд-АМДЗ» сле-дующих условий*:

1. На ПЭВМ (PC) с проверенным BIOS установлена проверенная операционная среда.

2. Достоверно установлена неизменность ОС, BIOS и программ для данного сеанса работы.
3. Кроме проверенных программ в данной программно-аппаратной среде ПЭВМ (PC) не запускалось и не запускается никаких иных программ.
4. Исключен запуск проверенных программ в какой-либо иной ситуации, т.е. вне проверенной среды при установленном специальном ПО СЗИ НСД.
5. Условия 1-4 выполняются в любой момент времени для всех пользователей, аутентифицированных защитным механизмом комплекса.

*При выполнении перечисленных условий программная среда называется изолированной (в терминах описания СЗИ НСД «Аккорд» используется термин ИПС – изолированная программная среда).

Особенности защитных функций

Особенностью СЗИ НСД «Аккорд-АМДЗ» является проведение процедур идентификации, аутентификации и контроля целостности до загрузки операционной системы. Это обеспечивается перехватом управления контроллером комплекса во время, так называемой, процедуры ROMscan, суть которой заключается в следующем:

В процессе начального старта после проверки основного оборудования BIOS ПЭВМ (PC) начинает поиск внешних ПЗУ в диапазоне от C800:0000 до E000:0000 с шагом в 2К. Признаком наличия ПЗУ является наличие слова AA55h в первом слове проверяемого интервала. Если данный признак обнаружен, то в следующем байте содержится длина ПЗУ в страницах по 512 байт. Затем вычисляется контрольная сумма всего ПЗУ, и если она корректна – будет произведен вызов процедуры, расположенной в ПЗУ со смещением 3. Такая процедура обычно используется для инициализации.

В СЗИ НСД «Аккорд-АМДЗ» в этой процедуре проводится идентификация и аутентификация пользователя. При ошибке возврат из процедуры не происходит, т.е. дальнейшая загрузка выполняться не будет.

Вся процедура идентификации и аутентификации занимает 7-10 секунд. Ее устойчивость зависит от длины пароля. Допускается установка пароля до 12 символов. Возможность установки длины пароля предоставляется только администратору безопасность информации (БИ).

При касании съемника информации персональным идентификатором пользователя осуществляется поиск предъявленного идентификатора в спи-

ске зарегистрированных, который хранится в ЭНП контроллера. Если предъ-явленный идентификатор обнаружен в списке, то производится аутентифи-кация пользователя и контроль целостности установленных в ПЭВМ (PC) технических и программных средств по перечню, создаваемого для каждого пользователя при его регистрации администратором БИ.

Для проведения процедуры аутентификации предусмотрен режим ввода пароля в скрытом виде – в виде символов «*». Этим предотвращается возможность раскрытия личного пароля и использования утраченного (похищенного) идентификатора.

Основой для достижения надежного функционирования системы защиты является контроль целостности технических и программных средств ПЭВМ (PC) перед каждым сеансом работы пользователя. Этим обеспечивается защита от несанкционированных модификаций и внедрения разрушающих программных воздействий (закладок, вирусов и т.д.).

Контроль целостности в СЗИ НСД «Аккорд-АМДЗ» выполняется на аппаратном уровне (средствами контроллера комплекса) с использованием алгоритма пошагового (ступенчатого) контроля целостности, суть которого сводится к следующему – для контроля данных на i-м логическом уровне их представления для чтения требуется использование предварительно прове-ренных на целостность процедур i-1-го уровня.

При этом обеспечивается корректная работа комплекса с загрузчиками различных файловых систем (Boot-менеджерами), что позволяет обеспечить доверенную загрузку всех ОС и прикладного ПО при одновременной их ус-тановке на дисках или разделах дисков ПЭВМ (PC).

Программы, реализующие механизм контроля целостности комплекса, администрирования и аудит работы пользователей защищены от подделки и несанкционированной модификации за счет их хранения в энергонезависи-мой памяти контроллера комплекса.

При осуществлении контрольных процедур (идентификации, аутенти-фикации пользователя, проверке целостности) блокируется загрузка ОС с от-чуждаемых носителей (флоппи-диск, CD ROM, ZIP-drive).

Установка и настройка комплекса СЗИ НСД «Аккорд-АМДЗ»

Установка комплекса осуществляется в соответствии с требованиями эксплуатационной документации.

Установка комплекса СЗИ НСД «Аккорд-АМДЗ» включает:

1. Установку контроллера комплекса в свободный слот материнской платы ПЭВМ (РС).
2. Регистрацию пользователей и настройку защитных средств комплекса.
3. При установке специального ПО производится назначение пользователям прав на доступ к ресурсам ПЭВМ (АС).

Управление защитой информации

Создаваемая структура защиты информации в ПЭВМ (АС) при применении комплекса СЗИ НСД «Аккорд-АМДЗ» должна поддерживаться механизмом установления полномочий пользователям ПЭВМ (АС) и управлением их доступом к информации.

Для этого на предприятии (учреждении, фирме и т.д.) создается служба безопасности информации (СБИ) или назначается ответственное лицо (администратор безопасности информации), на которых возлагается разработка и ввод в действие организационно-правовых документов по применению ПЭВМ (РС) с внедренными средствами защиты комплекса «Аккорд-АМДЗ». Этими документами предусматривается ведение ряда учетных и объектовых документов (например, «Журнал учета выданных идентификаторов», «Инструкции по применению ПЭВМ с внедренными СЗИ «Аккорд» для различных категорий должностных лиц и др.).

Содержание отчета

Отчет должен содержать:

1. Основные теоретические сведения;
2. Описание ходы выполнения лабораторной работы с основными результатами и выводами.

Контрольные вопросы

1. Составной частью какой деятельности предприятия являются мероприятия по защите информации от НСД?
2. Каково предназначение ПАК СЗИ от НСД «Аккорд»?
3. Выполнение каких функций обеспечивает контроллер?

4. Что необходимо для эффективного применения комплекса и поддержания соответствующего уровня защищенности ПЭВМ и информационных ресурсов?
5. В виде каких взаимодействующих между собой подсистем можно представить средства разграничения доступа к ресурсам?
6. Что такое процедура идентификации?
7. Что такое процедура аутентификации?
8. Что означает использование дискреционного принципа управления доступом?
9. Что означает использование мандатного принципа управления доступом?
10. Для чего предназначена подсистема регистрации и учета?
11. Что фиксируется в системном журнале при регистрации событий?
12. Для чего предназначена подсистема обеспечения целостности?
13. Что такое проверка на целостность?
14. Какие средства называются аппаратными?
15. Что такое несанкционированный доступ?
16. Что происходит при непосредственном несанкционированном доступе?
17. Что означает опосредованный несанкционированный доступ?
18. Что понимается под аббревиатурой АМДЗ?
19. Какие задачи возлагаются на службу безопасности информации?
20. Какие задачи решает администратор БИ при эксплуатации комплекса?
21. На основании чего реализованы защитные механизмы в СЗИ «Аккорд»?
22. В чем заключаются условия создания изолированной программной среды?
23. Чем определяется стойкость процедур идентификации и аутентификации?
24. Что может выступать дополнительными механизмами защиты от НСД к ПЭВМ?
25. Какие требования предъявляются к реализации дискреционного механизма разграничения доступа?
26. Для чего предназначена программа ACED32.EXE?
27. Какова максимальная длина пароля?
28. Что предусматривает статический режим контроля целостности файлов?
29. Что предусматривает динамический режим контроля целостности файлов?
30. Какой программой реализуется разграничение доступа пользователей к ресурсам компьютера?

ЛАБОРАТОРНАЯ РАБОТА № 9

Тема: Тестовые испытания программных средств защиты.

Цель работы

Применение методов и технологий испытания программного и аппаратного уровней комплексной защиты информации для проверки наличия и работоспособности встроенных программных и иных средств защиты КИС.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Изучить соответствующий теоретический материал по теме лабораторной работы.
3. Провести проверку, реализующую поставленную задачу.
4. Проанализировать проделанную работу и предложить возможный метод противодействия проверке.
5. Результат с рекомендациями по защите анализируемой ПЭВМ отразить в отчете.

Краткие теоретические сведения

Механизм очистки памяти защищает систему от восстановления удаленных конфиденциальных данных. Для проверки необходимо установить наличие в ПЭВМ специализированного программного обеспечения. Создать контрольный файл и уничтожить его.

Возможные программы восстановления: EasyRecovery, Filerecovery, Recover4all и др

Возможные программы гарантированного удаления: Acronis Privacy Expert Suite, Acronis Drive Cleanser, Systerac XP Toolls Shreder, Paragon Disc Wiper и др.

Механизм обеспечения целостности защищает среду обработки конфиденциальной информации от изменения данных и логики работы исполняе-мых файлов, от внедрения разрушающих программных средств, от подмены

информации. Для проверки требуется проанализировать ПЭВМ на наличие специализированного ПО. Создать контрольный файл и модифицировать его.

Возможные программы обеспечения целостности: Tripwire ASR, Symantec Enterprise Security Manager, IBM Tivoli Business Service Manager, Аккорд, ФПСУ X25 ACCESS TM-SHELL.

Аналогично вышеизложенному провести проверки испытуемой ПЭВМ на наличие механизмов: управления потоками информации, шифрования, контроля безопасности и аудита, обеспечения безопасности при взаимодействии с сетями общего пользования, сигнализации попыток нарушения защиты, антивирусной защиты, управления сертификатами, идентификации и аутентификации субъектов доступа, контроля доступа к ресурсам, регистрации и учета событий.

Содержание отчета

Отчет должен содержать:

1. Описание проверки.
2. Алгоритм, функциональная схема и функциональный состав проверки.
3. Вывод, в котором предлагаются методы повышения защищенности КИС.

Контрольные вопросы

1. В чем состоят источники угроз потокам информации?
2. В чем состоят источники угроз во взаимодействии с сетями общего пользования?
3. В чем состоят источники угроз при отсутствии контроля доступа к инфоресурсам?
4. Раскройте понятие обнаружение атак.
5. В чем состоит сложность использования механизма шифрования?
6. В чем заключаются слабости решения с помощью организационных методов защиты?
7. Приведите несколько примеров применения механизма регистрации и учета событий.
8. Расскажите о методах противодействия указанным проверкам.

ЛАБОРАТОРНАЯ РАБОТА № 10

Тема: Защита от утечек по каналу ПЭМИН, по акустическому и виброакустическому каналам.

Цель работы

Применение методов и технологий испытания аппаратного уровня комплексной защиты информации.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Провести проверку, реализующую поставленную задачу.
3. Проанализировать проделанную работу и предложить возможный метод противодействия проверке.
4. Результат и рекомендации по защите отразить в отчете.

Краткие теоретические сведения

Защита информации от утечки по техническим каналам – это комплекс организационных, организационно-технических и технических мероприятий, исключающих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны.

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

В основе утечки конфиденциальной информации по техническим каналам лежит неконтролируемый перенос ценных сведений посредством акустических, электромагнитных, радиационных и других полей и материальных объектов. Причиной утечки является несовершенство норм по сохранению информации в аппаратных средствах, а также нарушение указанных норм.

Защита информации от утечки по акустическому и виброакустическому каналу предполагает применение архитектурно-планировочных, пространственных, режимных, пассивных (звукоизоляция) и активных (звукоподавление) мероприятий.

Тестовые испытания защиты информации от утечки по акустическому и виброакустическому каналам включают:

– измерение звукоизоляции выделенных помещений;

– измерение виброизоляции выделенных помещений;

– измерение электроакустических преобразований вспомогательных технических средств.

Защита от утечки за счет паразитных электромагнитных излучений и наводок (ПЭМИН) требует строгого исполнения порядка размещения аппа-ратных средств в пространстве объекта и относительно друг друга.

Тестовые испытания защиты информации от утечки за счет наводок и ПЭМИ включают:

– измерение ПЭМИ рабочих станций (АРМ) пользователей, серверов, уст-ройств вывода (ввода) информации, коммуникационного оборудования и ка-бельных соединений;

– измерение наводок информационных сигналов на вспомогательные средства, имеющие выход за пределы контролируемой зоны;

– измерение наводок информационных сигналов на кабельное и коммуникационное оборудование.

Проверку эффективности защиты по указанным каналам проводят с применением шумомера, электронного стетоскопа, селективного нановольт-метра, измерительного приемника, анализатора спектра и иных специализи-рованных измерительных приборов.

Канал утечки информации состоит из источника сигнала, физической среды его распространения и приемной аппаратуры на стороне злоумышлен-ника. Движение информации в таком канале осуществляется только в одну сторону — от источника к злоумышленнику. На рисунке 15 приведена струк-тура канала утечки информации.

Рис.15. Структура канала утечки информации

Под каналом утечки информации будем понимать физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка или несанкционированное получение охраняемых сведении. Для возникновения (образования, установления) канала утечки инфор-мации необходимы определенные пространственные, энергетические и вре-менные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

Применительно к практике с учетом физической природы образования каналы утечки информации можно квалифицировать на следующие группы:

– визуально-оптические;
– акустические (включая и акустико-преобразовательные);
– электромагнитные (включая магнитные и электрические);
– материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида – твердые, жидкие, газообразные).

Для выполнения работы по проверке провести необходимые измерения с использованием объекта проверки и измерительных приборов по выбору преподавателя.

Содержание отчета

Отчет должен содержать:

1. Описание проверки.
2. Алгоритм, функциональная схема и функциональный состав проверки.
3. Вывод, в котором предлагаются методы повышения защищенности аппаратной части КИС.

Контрольные вопросы

1. Перечислите виды возможных технических каналов утечки информации.
2. Раскройте понятие акустоэлектрический канал утечки информации.
3. Какова роль акустического канала в общем перечне возможных каналов утечки?
4. Какие средства позволяют реализовать защиту по каналу ПЭМИН?
5. Приведите несколько примеров пассивной защиты выделенного помещения.
6. Как замаскировать виброакустический канал утечки конфиденциальной информации?

7. Расскажите о методах противодействия указанным проверкам.
8. Какие недостатки присущи проверке по каналу ПЭМИН?

ЛАБОРАТОРНАЯ РАБОТА № 11

Тема: Анализ сетевой топологии и установленных сервисов

Цель работы

Применение методов и технологий испытания программного и аппа-ратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Изучить соответствующий теоретический материал по курсу «Вычислительные сети».
3. Провести проверку, реализующую поставленную задачу.
4. Проанализировать проделанную работу и предложить возможный метод противодействия атаке.
5. Результат с рекомендациями по защите анализируемой сети и ПЭВМ отразить в отчете.

Краткие теоретические сведения

Информация о топологии сети имеет значение как для учета ее ресурсов, диагностирования отказов в работе сети, планирования развития сети, так и планирования атаки злоумышленником на КИС.

Для реализации проверки путем «дружественного» взлома требуется проведение анализа топологии сети, определение внутренней доменной структуры и установленных сервисов. В том числе определяются средства межсетевого экранирования, признаки работы сервисов по нестандартным портам и типы примененных операционных систем.

С указанной выше целью возможен перехват пакетов сетевого управ-ления (например пакет HP Open View Network Node Manager), дающий ин-

формацию о топологии на 3 уровне модели OSI. Для 2 уровня актуальны фирменные протоколы, использующие расширения технологии SNMP. В том числе протоколы: CDP, EDP, NDP. Фирмой Loran Networks применен метод фрактальных сопоставлений. Исследование доменной структуры проводится с использованием службы каталогов Active Directory.

Методы выявления средств МСЭ основываются на анализе информации о взаимодействии. Наиболее часто применяются возможности протокола ICMP, разведка с помощью DNS-служб, обнаружение фильтрации и блокировки трафика на основе диапазонов адресов.

Основным методом определения работы сервисов по нестандартным портам является их полное сканирование и проведение анализа заголовков ответов.

Для установления типа используемой операционной системы применим анализ реакции различных операционных систем на одинаковый запрос. Исследовав особенности реакции заранее известных операционных систем на запрос, возможно, набрать определенную статистику. Комбинируя воздействие, конкретизируем статистическую информацию.

Содержание отчета

Отчет должен содержать:

1. Описание атак по анализу топологии сети, определению внутренней доменной структуры и установленных сервисов. Определению средств межсетевого экранирования, признаков работы сервисов по нестандартным портам и типов примененных операционных систем.
2. Алгоритм, функциональная схема и функциональный состав программы.
3. Вывод, в котором предлагаются решения повышения защищенности КИС.

Контрольные вопросы

1. Перечислите источники информации о топологии сети.
2. В чем заключается угроза раскрытия информации DNS служб?
3. Что положено в основу определения работы сервисов по нестандартным портам?
4. Раскройте понятие «реакция на запрос ОС».

5. Какова роль службы каталогов Active Directory в обеспечении защиты (Windows 2000, XP)?
6. Расскажите о методах противодействия данным атакам.

ЛАБОРАТОРНАЯ РАБОТА № 12

Тема: Сетевое сканирование

Цель работы

Применение методов и технологий испытания программного и аппа-ратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Изучить соответствующий теоретический материал по теме лабораторой работы.
3. Провести проверку, реализующую поставленную задачу.
4. Проанализировать проделанную работу и предложить возможный метод противодействия атаке.
5. Результат с рекомендациями по защите анализируемой сети и ПЭВМ отразить в отчете.

Краткие теоретические сведения

Сканирование как метод раскрытия каналов передачи данных существует достаточно давно. Его идея заключается в том, чтобы исследовать наибольшее количество каналов и отслеживать те из них, которые находятся в состоянии ожидания соединения и, следовательно, могут быть использованы злоумышленником.

Сам по себе термин "сканирование" появился в процессе слияния ком-пьютеров с телефонными системами. В результате была сформирована гло-бальная сеть телефонных коммуникаций, доступ в которую можно получить, всего лишь набрав номер на телефонном аппарате. С одного телефона дос-

тупны миллионы абонентов телефонной сети, однако полезными могут оказаться лишь сотни, а то и десятки абонентов, к телефонам которых подклю-чен модем. Логически верным подходом для поиска телефонных номеров та-ких абонентов является "атака в лоб" - перебор всех возможных номеров АТС и поиск тона несущей частоты, генерируемого модемом на другом кон-це линии. Так возникло направление, называемое wardialing.

Wardialing является весьма эффективным методом для поиска входов в различные сети по коммутируемой телефонной линии. С другой стороны, ог-ромное число компьютеров объединены в сеть с помощью специального оборудования (сетевых адаптеров, кабельных модемов) и выделенных линий и не используют коммутируемые линии АТС.

Термин "порт" является абстрактным понятием, используемым для упрощенного описания механизма установления соединения между хостами, и представляет собой потенциальный канал передачи данных. Использование механизма портов существенно облегчает процесс установления соединения и обмена информацией между сервером и хостом. Кроме того, имеется воз-можность исследования сетевого окружения сервера методом опроса его портов (т.н. "сканирование" портов). На все возможные номера портов (1-65535) сервера посылается "лавина" пакетов, и по тому, от каких портов бу-дут (или не будут) получены ответы, определяются открытые порты и служ-бы, работающие на исследуемом сервере.

Для реализации проверки путем «дружественного» взлома требуется проведение сетевого сканирования, что позволит провести подробный анализ сети и установленных сервисов. С этой целью проводится сетевое сканиро-вание и определение установленных сервисов, которое включает:

- сканирование TCP-портов функцией connect;
- сканирование с использованием ICMP echo-пакетов;
- SYN-сканирование TCP-портов;
- FIN-сканирование TCP-портов;
- сканирование с использованием фрагментации;
- обратное IDENT-сканирование;
- FTP bounce-сканирование;
- UDP-сканирование;

- определение списка открытых и закрытых портов;
- определение списка имеющихся средств межсетевого экранирования;

– определение признаков работы сервисов по нестандартным портам;
– определение типов используемых операционных систем.

Содержание отчета

Отчет должен содержать:

1. Описание атак по анализу топологии сети, определению внутренней доменной структуры и установленных сервисов. Определению средств межсетевого экранирования, признаков работы сервисов по нестандартным портам и типов примененных операционных систем.
2. Алгоритм, функциональная схема и функциональный состав проверки.
3. Вывод, в котором предлагаются решения повышения защищенности КИС.

1. Контрольные вопросы

1. В чем состоят источники угроз сканирования?
2. Перечислите возможные направления сканирования.
3. Раскройте понятие FTP-сканирования.
4. В чем состоит сложность использования обратного IDENT сканирования?
5. В чем заключаются слабости решения с помощью FTP bounce сканирования?
6. Приведите несколько примеров применения сканирования.
7. Расскажите о методах противодействия данной атаке.

ЛАБОРАТОРНАЯ РАБОТА № 13

Тема: Анализ трафика и сбор критичной информации программами пассивного анализа

Цель работы

Применение методов и технологий испытания программного и аппа-ратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Изучить соответствующий теоретический материал по теме лабораторной работы.
3. Провести проверку, реализующую поставленную задачу.
4. Проанализировать проделанную работу и предложить возможный метод противодействия атаке.
5. Результат с рекомендациями по защите анализируемой сети и ПЭВМ отразить в отчете

Краткие теоретические сведения

Анализ трафика и сбор критичной информации программами пассивного анализа является одним из методов получения критичной информации о корпоративной информационной системе.

Для реализации необходимо иметь специализированное программное обеспечение.

В сфере обеспечения ИБ необходимо обнаруживать и нейтрализовать вредоносный код прежде, чем он нанесет ущерб информационной системе. Проанализировав нестандартное «поведение» трафика, можно определить его как угрожающее и, блокировав действие соответствующих программ, со-общить пользователю об инциденте.

Проведение анализа трафика и сбор критичной информации с применением программ пассивного анализа (программ-снифферов и программ об-наружения вторжений) включает:

– получение информации об используемых аутентификационных протоколах, процедурах доступа;
– обнаружение в открытом трафика передаваемых регистрационных имен,
– идентификаторов и паролей пользователей, определение текстовых паролей, паролей на доступ в удаленные системы;
– проверка паролей, используемых при аутентификации службами SMB, POP3, IMAP, Telnet, HTTP, FTP и др.;
– определение почтовых ящиков на общедоступных почтовых серверах;
– анализ почтового трафика на предмет выявления писем, отвечающих оп-

ределенным признакам;

- диагностика проблем при сетевом обмене хостов;
- проверочная рассылка электронной почты со служебными заголовками;
- определение свойств реализации стека TCP;
- определение маршрутов хождения пакетов;
- тестирование правильности настроек систем контроля трафика.

Содержание отчета

Отчет должен содержать:

1. Описание атак по анализу топологии сети, определению внутренней доменной структуры и установленных сервисов. Определению средств межсетевого экранирования, признаков работы сервисов по нестандартным портам и типов примененных операционных систем.
2. Алгоритм, функциональная схема и функциональный состав проверки.
3. Вывод, в котором предлагаются решения повышения защищенности КИС.

Контрольные вопросы

1. В чем заключается угроза пассивного анализа?
2. Что положено в основу атаки?
3. Раскройте понятие «трафик» в вычислительной системе.
4. Какова роль анализа трафика системе?
5. Какие средства позволяют реализовать пассивный анализ?
6. Расскажите о методах противодействия данной атаке.
7. Какие недостатки присущи пассивному анализу?

ЛАБОРАТОРНАЯ РАБОТА № 14

Тема: Обнаружение уязвимостей по сигнатурам

Цель работы

Применение методов и технологий испытания программного и аппа-ратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Изучить соответствующий теоретический материал по теме лабораторной работы.
3. Провести проверку, реализующую поставленную задачу.
4. Проанализировать проделанную работу и предложить возможный метод противодействия атаке.
5. Результат с рекомендациями по защите анализируемой сети и ПЭВМ отразить в отчете.

Краткие теоретические сведения

Обнаружение уязвимостей по сигнатурам является одним из методов получения критичной информации о корпоративной информационной систе-ме.

Для реализации необходимо иметь специализированное программное обеспечение. Обнаружение имеющихся уязвимостей по имеющимся сигна-турам включает:

– определение слабых мест в защите сервисов: FTP, TFTP, SSH, Finger, HTTP, IMAP SMTP, NetBIOS/SMB, RPC;
– выявление слабых мест сетевых информационных служб (NIS);
– проверка на возможность IP-спуфинга;
– проверка маршрутизации из источника rlogin, rsh и telnet;
– проверка IP-переадресации (forwarding);
– проверка сетевых масок и временных меток (timestamp) ICMP;
– проверка инкапсуляции пакета MBONE;
– проверка инкапсуляции APPLETALK IP, IPX, X.25, FR;
– проверки резервированных разрядов и паритет-протоколов;
– проверка специализированных фильтров;
– проверка фильтров с возможностью нулевой длины TCP и IP;
– проверка на передачу сверхнормативных пакетов;
– проверка опций post-EOL для TCP и IP;
– проверка наличия в Web-сервисах уязвимых сценариев, на базе Basic

Script, JavaScript, Perl и ActiveXo;

– проверка программного обеспечения на закрытие всех известных уязвимостей данной платформы.

Содержание отчета

Отчет должен содержать:

1. Описание атак по анализу топологии сети,
2. Описание определения внутренней доменной структуры и установленных сервисов.
3. Описание определения средств межсетевого экранирования, признаков работы сервисов по нестандартным портам и типов примененных операционных систем.
4. Алгоритм, функциональная схема и функциональный состав проверки.
5. Вывод, в котором предлагаются решения повышения защищенности КИС.

Контрольные вопросы

1. В чем заключается угроза уязвимости по сигнатурам?
2. Что положено в основу определения уязвимости по сигнатурам?
3. Раскройте понятие «Сигнатура» в контексте защиты информации в вычислительной системе.
4. Какова роль сигнатуры в операционной системе?
5. Какие средства позволяют реализовать атаку на уязвимость?
6. Расскажите о методах противодействия данной атаке.

ЛАБОРАТОРНАЯ РАБОТА № 15

Тема: Оценка уязвимости коммутируемого доступа

Цель работы:

Применение методов и технологий испытания программного и аппа-ратного уровней комплексной защиты информации для проведения атаки на КИС с целью установления уязвимостей.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Изучить соответствующий теоретический материал по теме лабораторной работы.
3. Провести проверку, реализующую поставленную задачу.
4. Проанализировать проделанную работу и предложить возможный метод противодействия атаке.
5. Результат с рекомендациями по защите анализируемой сети и ПЭВМ отразить в отчете

Краткие теоретические сведения

Оценка уязвимости коммутируемого доступа в вычислительную сеть предприятия является одним из методов получения критичной информации о корпоративной информационной системе.

Для реализации необходимо иметь специализированное программное обеспечение.

Уязвимость – слабое место в информационной системе, которое может привести к нарушению безопасности. Различают человеческую уязвимость и техническую уязвимость, возникающая в результате неисправности техноло-гического компонента информационной системы.

Коммутируемый доступ – в коммуникационных сетях - доступ, при котором обеспечивается установление соединений только по необходимости.

Оценка уязвимости коммутируемого доступа включает:

– определение каналов удаленного доступа с коммутируемым подключением, которые могут быть использованы для вхождения во внутреннюю сеть через телефонные сети общего пользования;

– анализ защищенности каналов удаленного доступа с коммутируемым подключением.

Содержание отчета

Отчет должен содержать:

1. Описание атак на коммутируемый доступ к сети
2. Алгоритм, функциональная схема и функциональный состав проверки.

3. Вывод, в котором предлагаются решения повышения защищенности КИС.

Контрольные вопросы

1. Перечислите виды коммутируемого доступа.
2. Раскройте понятие коммутируемый доступ.
3. В чем состоит сложность использования коммутируемого доступа?
4. В чем заключаются слабости коммутируемого доступа ?
5. Приведите несколько примеров применения уязвимости коммутируемого доступа.
6. Расскажите о методах противодействия данной атаке.

ЛАБОРАТОРНАЯ РАБОТА № 16

Тема: Анализ угроз и рисков комплексной защиты информации на объекте с использованием системы «Гриф»

Цель работы

Применение принципов организации, проектирования и анализа систем защиты информации и основ их комплексного построения на различных уровнях защиты.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Выполнить работу по анализу угроз и рисков с использованием системы «Гриф».
3. Проанализировать проделанную работу и предложить метод внедрения системы «Гриф» на предприятии.
4. Результат отразить в отчете.

Краткие теоретические сведения

Троянская программа должна без потерь копировать файлы произволь-ной длины и любым расширением. Дополнительным заданием может слу-

жить создание программы, которая делала бы точную копию системы каталогов пользователя А.

Программные средства, позволяющие провести полный анализ рисков, строятся с использованием структурных методов системного анализа и про-ектирования (SSADM – Structured Systems Analysis and Design) и представ-ляют собой инструментарий для:

– построения модели ИС с точки зрения ИБ;
– оценки ценности ресурсов;
– составления списка угроз и уязвимостей, оценки их характеристик;
– выбора контрмер и анализа их эффективности;
– анализа вариантов построения защиты;
– документирования (генерация отчетов).

Примерами программных продуктов этого класса являются CRAMM, разработчик Logica (Великобритания), MARION, разработчик CLUSIF (Франция), RiskWatch (США), ГРИФ, разработчик Digital Security.

Обязательным элементом этих продуктов является база данных, содержащая информацию по инцидентам в области ИБ, позволяющая оценить риски и уязвимости, эффективность различных вариантов контрмер в опре-деленной ситуации.

Принципы, положенные в основу методик анализа рисков и границы их применимости. Один из возможных подходов к разработке подобных мето-дик – накопление статистических данных о реально случившихся происше-ствиях, анализ и классификация их причин, выявление факторов риска. На основе этой информации можно оценить угрозы и уязвимости в других ин-формационных системах.

Практические сложности в реализации этого подхода следующие:

– Во-первых, должен быть собран весьма обширный материал о происшествиях в этой области.
– Во-вторых, применение этого подхода оправдано далеко не всегда.

Если информационная система достаточно крупная (содержит много элементов, расположена на обширной территории), имеет давнюю историю, то подобный подход, скорее всего, применим.

Если система сравнительно невелика, использует только новейшие элементы технологии (для которых пока нет достоверной статистики), оцен-ки рисков и уязвимостей могут оказаться недостоверными.

Содержание отчета

Отчет должен содержать:

1. Описание организации проведения анализа угроз и рисков на предприятии.
2. Формальный отчет по результатам анализа.
3. Вывод, в котором предлагаются методы решения проблемы защиты информации.

Контрольные вопросы

1. В чем заключается угроза раскрытия информации? Какие еще угрозы Вы знаете?
2. Что положено в основу системы «Гриф»?
3. Какова роль руководителя системе «Гриф»?
4. Какие средства позволяют реализовать систему «Гриф» на предприятии?
5. Приведите несколько примеров расчета рисков при изменении системы защиты информации.
6. Какие недостатки присущи системе «Гриф»?

ЛАБОРАТОРНАЯ РАБОТА № 17

Тема: Анализ и управление политикой информационной безопасности на объекте с использованием системы «Кондор»

Цель работы

Применение принципов организации, проектирования и анализа систем защиты информации и основ их комплексного построения на различных уровнях защиты.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Выполнить работу по анализу угроз и рисков с использованием системы «Кондор».

3. Проанализировать проделанную работу и предложить метод внедрения системы «Кондор» на предприятии.
4. Результат отразить в отчете.

Краткие теоретические сведения

Для реализации анализа состояния ИБ предприятия и построения системы ее управления рекомендуется применять специализированное программное обеспечение.

Система «Кондор» позволяет с минимальным привлечением сторонних сил и средств проанализировать состояние ИБ предприятия и построить адекватную угрозам систему управления ИБ предприятия.

Для того чтобы обеспечить базовый уровень безопасности, достаточно проверить выполнение требований соответствующего стандарта (специфика-ции), *например* ISO 17799.

Программные продукты анализа рисков для базового уровня информационной безопасности, позволяют сформировать список вопросов, касаю-щихся выполнения этих требований. На основе ответов генерируется отчет с рекомендациями по устранению выявленных недостатков.

Примером программного продукта этого класса является система «Кондор».

Данное программное обеспечение позволяет существенно облегчить процесс проверки на соответствие требованиям Британского стандарта BS 7799 (ISO 17799) информационной системы.

Имеется несколько баз знаний:

– общие требования BS 7799 (ISO 17799),

– специализированные базы, ориентированные на различные области применения.

Содержание отчета

Отчет должен содержать:

1. Описание организации проведения анализа и управления информационной безопасности на предприятии.
2. Формальный отчет по результатам анализа.
3. Вывод, в котором предлагаются методы решения проблемы защиты информации.

Контрольные вопросы

1. Перечислите источники угроз безопасности информации предприятия.
2. В чем заключается угроза НСД?
3. Что положено в основу санкционированного доступа?
4. Раскройте понятие «Управление политикой безопасности» в контексте защиты информации в вычислительной системе.
5. Какие средства позволяют реализовать систему «Кондор»?
6. Какие недостатки присущи системе «Кондор»?

ЛАБОРАТОРНАЯ РАБОТА № 18

Тема: Аудит комплексной защиты информации предприятия

Цель работы

Применение принципов организации, проектирования и анализа систем защиты информации и основ их комплексного построения на различных уровнях защиты.

Подготовка и порядок выполнения работы

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Выполнить работу по аудиту комплексной защиты информации предприятия.
3. Проанализировать проделанную работу и предложить свой метод проведения аудита комплексной защиты информации на предприятии.
4. Результат отразить в отчете.

Краткие теоретические сведения

Аудит комплексной защиты информации является основой построения системы защиты информации предприятия. Для его проведения и получения достоверных результатов требуется, как правило, привлечение сторонних специализированных организаций.

При создании любой информационной системы (ИС) на базе современ-ных компьютерных технологий неизбежно возникает вопрос о защищенно-

сти этой системы от внутренних и внешних угроз безопасности информации. Но прежде чем решить, как и от кого защищать информацию, необходимо уяснить реальное положение в области обеспечения безопасности информа-ции на предприятии и оценить степень защищенности информационных ак-тивов.

Для этого проводится комплексное обследование защищенности ИС (или аудит безопасности), основанные на выявленных угрозах безопасности информации и имеющихся методах их парирования, результаты которого позволяют:

1. оценить необходимость и достаточность принятых мер обеспечения безопасности информации;
2. сформировать политику безопасности;
3. правильно выбрать степень защищенности информационной системы;
4. выработать требования к средствам и методам защиты;
5. добиться максимальной отдачи от инвестиций в создании и обслуживании СОБИ.

Комплексное обследование (аудит безопасности информации) защи-щенности представляет собой системный процесс получения и оценки объ-ективных данных о текущем состоянии обеспечения безопасности информа-ции на объектах информатизации, действиях и событиях, происходящих в информационной системе, определяющих уровень их соответствия опреде-ленному критерию.

Комплексное обследование защищенности ИС (аудит) позволяет оценить реальное положение в области защиты информации и принять комплекс обоснованных управленческих решений по обеспечению необходимого уровня защищенности информационных активов предприятия.

Аудит защищенности ИС ставит своей целью методологическое обсле-дование процессов, методов и средств обеспечения безопасности информа-ции при выполнении информационной системой своего главного предназна-чения – информационное обеспечение бизнеса. При этом предполагается, что сама информационная система является оптимальной для решения бизнес –задач.

Результатом аудита защищенности могут быть рекомендации по изме-нению инфраструктуры сети, когда по экономическим соображениям нецеле-сообразно или невозможностью достичь требуемого уровня защищенности

информации при существующей инфраструктуре ИС.

Поскольку информационная безопасность должна быть обеспечена не только на техническом, но и на организационно-административном уровне, должный эффект может дать только комплексный подход к обследованию (аудиту), то есть:

1. проверка достаточности принятых программно-аппаратных и технических мер защиты (соответствие установленным требованиям применяемых в ИС программно-аппаратных средств защиты);
2. проверка достаточности инженерно-технических, правовых, экономических и организационных мер защиты (физической защиты, работы с персоналом, регламентации его действий).

Целью проведения работ по комплексному обследованию защищенности ИС является получение объективных данных о текущем состоянии обеспечения безопасности информации на объектах ИС, позволяющих провести минимизацию вероятности причинения ущерба собственнику информационных активов в результате нарушения конфиденциальности, целостности или доступности информации, подлежащей защите, за счет получения несанкционированного доступа к ней, а также выработка комплекса мер, направленных на повышение степени защищенности информации ограниченного доступа.

Процесс комплексного обследования защищенности информационной системы состоит из трех основных частей:

1. сбор необходимых исходных данных и их предварительный анализ (или стадия планирования);
2. оценка соответствия состояния защищенности ИС предъявляемым требованиям и стандартам (стадии моделирования, тестирования и анализа результатов);
3. формулирование рекомендаций по повышению безопасности информации в обследуемой ИС (стадии разработки предложений и документирования полученных результатов).

На разных этапах обследования используются различные методы: тех-нические, аналитические, экспертные, расчетные. При этом, результаты, по-лученные одними методами, могут дублироваться (дополняться) результата-ми, полученными другими методами. Совокупность всех применяемых мето-дов позволяет дать объективную оценку состояния обеспечения безопасности

информации на обследуемом объекте.

Основными группами методов при обследовании являются:

1. Экспертно-аналитические методы предусматривают проверку соответствия обследуемого объекта установленным требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации, а также соответствия реальных условий эксплуатации оборудования предъявляемым требованиям по размещению, монтажу и эксплуатации технических и программных средств.
2. Экспертно-инструментальные методы предполагают проведение проверки функций или комплекса функций защиты информации с помощью специального инструментария (тестирующих средств) и средств мониторинга, а также путем пробного запуска средств защиты информации и наблюдения реакции за их выполнением. В процессе испытаний технических и программных средств используются тестирующие средства, принятые в установленном порядке.
3. Моделирование действий злоумышленника («дружественный взлом» системы защиты информации) применяются после анализа результатов, полученных в ходе использования первых двух групп методов, – они необходимы как для контроля данных результатов. Этим методом подтверждаются также реальные возможности потенциальных злоумышленников (как внутренних, легально допущенных к работе с тем или иным уровнем привилегий в ИС, так и внешних – в случае подключения ИС к глобальным информационным сетям). Кроме того, подобные методы могут использоваться для получения дополнительной исходной информации об объекте, которую не удалось получить другими методами.

Важным моментом является то, что применение методов моделирования действий злоумышленника ограниченно. При использовании данных методов необходимо учитывать, что при осуществлении тестовой атаки, используемое в ИС оборудование может быть выведено из строя, информационные ресурсы утрачены или искажены.

Содержание отчета

Отчет должен содержать:

1. Описание организации проведения Аудита на предприятии.

2. Формальный отчет по результатам Аудита.
3. Вывод, в котором предлагаются методы решения проблемы защиты информации.

Контрольные вопросы

1. Кратко сформулируйте виды Аудита КЗИ.
2. В чем состоят источники успеха Аудита?
3. Раскройте понятие «Сюрвей».
4. В чем состоит сложность применения Аудита КЗИ?
5. В чем заключаются слабости внутреннего Аудита силами предприятия?
6. Приведите несколько примеров успешного применения Аудита.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Абалмазов, Э.И. Энциклопедия безопасности. Часть 1. Оружие шпионажа: эл. учеб. пос/ Э. И. Абалмазов. – 1997 г. www.kiev-security.org.ua
2. Абалмазов, Э.И. Методы и инженерно-технические средства противодействия информационным угрозам/ Э. И. Абалмазов. – М.: Изд-во “Компания “Гротек”, 1997 г. – 246 с.
3. Баранов, А.П. Математические основы информационной безопасности: учеб. пособие/ А.П. Баранов, Н.П. Борисенко, П.Д. Зегжда, и др. – Орел: ВИПС, 1997. – 354 с.
4. Большая энциклопедия промышленного шпионажа/ Ю.Ф. Каторин Ю.Ф. и др.. – СПб.: ООО “Изд-во “Полигон”, 2000. – 896 с.
5. Гарсиа, М. Проектирование и оценка систем физической защиты. Опера-ционные системы. Основы и принципы: Третье издание. Пер. с англ. – М.: Мир, 2003г. – 386 с.
6. Завгородний, В.И. Комплексная защита информации в компьютерных системах. М.: Логос, 2001. – 264 с.
7. Зайцев, А.П. Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации/ А.П. Зайцев, А.А. Ше-лупанов. – Томск: ТУСУР, 2004. – 204 с.
8. Зима, В.М. Безопасность глобальных сетевых технологий/ В.М. Зима, А.А. Молдовян, Н.А. Молдовян. – Спб: БХВ-Петербург, 2000. – 368 с.
9. Информационная безопасность: сборник методических материалов/ отв. за выпуск М.М. Кучеров, Т.М. Пестунова. – М.: ФГУП «ЦНИИАТОМИН-ФОРМ», 2003. – 112 с.
10. Корт, С.С. Теоретические основы защиты информации: учеб. пособие/ С.С. Корт. – М.: Гелиос АРВ, 2004. – 240 с.
11. Кучеров, М.М. Язык Си: учеб. пособие для студентов направления 552800 – «Информатика и вычислительная техника»/ М.М. Кучеров. – Красноярск: КГТУ, 1994. – 87 с.
12. Лукацкий, А.В. Обнаружение атак. – СПб.: БХВ-Петербург, 2001. – 624 с.
13. Мельников, В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – 386 с.

14. Моторный, И.Д. Современный терроризм и оценка диверсионно-террористической уязвимости гражданских объектов. М: Издатель Шумило-ва И.И., 2004. – 106 с.
15. ПАК защиты компьютера от НСД Dallas Lock 4.1. Руководство администратора. – Спб: Конфидент, 1999. – 144 с.
16. Поздняков, Е.Н. Защита объектов: (Рекомендации для руководителей и сотрудников служб безопасности). М.: Концерн "Банк. деловой центр", 1997. – 222 с.
17. Радиоэлектронная разведка и радиомаскировка/ В.П. Демин и др. – М.: Изд-во МАИ, 1997. – 156 с.
18. Расследование неправомерного доступа к компьютерной информации / Под ред. Н.Г. Шурухнова. М.: Щит-М, 1999. – 254 с.
19. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. М.: Радио и связь, 1999. – 328 с.
20. Романец, Ю.В., Защита информации в компьютерных системах и сетях / Тимофеев, П.А., Шаньгин, В.Ф. – М.: Радио и связь, 1999. – 328 с.
21. Хореев, А.А. Защита информации от утечки по техническим каналам утечки информации. Часть 1. Технические каналы утечки информации/ А.А. Хорев. – М.: Гостехкомиссия России, 1998. – 320 с