

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования (ФГБОУ ВПО)
КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

Факультет прикладной информатики
Кафедра компьютерных технологий и систем

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

**Практикум для бакалавров специальности
«Бизнес-информатика»**

**Краснодар
2013**

Рецензенты:

- доктор технических наук, профессор Атрощенко В.А. – декан факультета компьютерных технологий и автоматизированных систем ФБГОУ ВПО "Кубанский государственный технологический университет";
- доктор экономических наук, профессор Луценко Е.В. – профессор кафедры компьютерных технологий систем ФБГОУ ВПО "Кубанский государственный аграрный университет".

Информационная безопасность: Практикум для бакалавров специальности «Бизнес-информатика». / В.Н. Лаптев, С.В. Лаптев. – Краснодар: КубГАУ, 2013. – 106 с.

Практикум по информационной безопасности подготовлен в соответствии с требованиями Государственных образовательных стандартов (ГОС) высшего профессионального образования для специальности «Бизнес-информатика» для бакалавров факультета прикладной информатики ФБГОУ ВПО "Кубанский государственный аграрный университет" (КубГАУ).

Он является обязательным приложением к курсу лекций по дисциплине «Информационная безопасность», так как обеспечивает проведение лабораторных занятий и выполнение самостоятельной работы студентами по учебному курсу. В работе рассмотрены теоретические и практические основы обеспечения защиты информации при проектировании и эксплуатации автоматизированных информационных систем, приемы работы пользователя с данными и информацией, аппаратно-программными и инженерно-техническими комплексами в защищенных компьютерных системах. Выполнение совокупности предложенных в практикуме сквозных практических заданий и подготовка ответов на контрольные вопросы обеспечит высокую эффективность обучения студентов работе в сфере информационной безопасности и защите информации.

Рассмотрены и рекомендованы к изданию на заседании кафедры компьютерных технологий и систем КубГАУ __ сентября 2013 г., протокол №1.

Рекомендованы к печати:

- Советом факультета прикладной информатики Кубанского государственного аграрного университета __ сентября 2013 г., протокол № __.

© Лаптев Владимир Николаевич, Лаптев Сергей Вдаимирович

© Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Кубанский государственный аграрный университет", 2013.

Оглавление

ВВЕДЕНИЕ	4
ЛАБОРАТОРНЫЕ ЗАНЯТИЯ.....	6
ЛЗ-01. РАЗРАБОТКА МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ	6
ЛЗ-02 РАЗГРАНИЧЕНИЕ ДОСТУПА К ИНФОРМАЦИИ В ОС WINDOWS	28
ЛЗ-03. КОНТРОЛЬ ЗА СОСТОЯНИЕМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ	37
ЛЗ-04. ИССЛЕДОВАНИЕ ПРОБЛЕМ ОЧИСТКИ МАГНИТНЫХ НОСИТЕЛЕЙ	47
ЛЗ-05. СРЕДСТВА ЗИ ОТ РАЗРУШАЮЩИХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ (РПВ).....	50
ЛЗ-06. ПРИМЕНЕНИЕ ПРОГРАММНЫХ АНТИВИРУСНЫХ КОМПЛЕКСОВ	54
ЛЗ-07. ИССЛЕДОВАНИЕ ПРОГРАММНЫХ СРЕДСТВ БОРЬБЫ С КОМПЬЮТЕРНЫМИ ВИРУСАМИ.....	66
ЛЗ-08. ПОСТРОЕНИЕ СЗИ НА ОСНОВЕ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ	71
ЛЗ-09. ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ	74
ЛЗ-10. АППАРАТНЫЕ СРЕДСТВА ОПОЗНАНИЯ ПОЛЬЗОВАТЕЛЕЙ.....	80
ЛЗ-11. СРЕДСТВА ЗАЩИТЫ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ ИНФОРМАЦИИ	88
ЛЗ-12. ИССЛЕДОВАНИЕ ПРОГРАММ, ЗАЩИЩЕННЫХ ОТ КОПИРОВАНИЯ	90
ЛЗ 15. УСТРОЙСТВО И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД И РАБОТА В СРЕДЕ СЗИ.....	94
ЛЗ-16. РАБОТА В СРЕДЕ СЗИ ОТ НСД “SECRET NET”	97
ЛЗ-17. ЗАЩИТА ИНФОРМАЦИИ В ЛВС NetWare	101
ЗАКЛЮЧЕНИЕ	105
ЛИТЕРАТУРА.....	106

ВВЕДЕНИЕ

Данный материал практикума собран на основании опыта преподавания дисциплины "Информационная безопасность и защита информации" в высших учебных заведениях для технических, экономических и юридических специальностей в соответствии с требованиями их учебных планов, основных образовательных программ профессиональной подготовки специалистов и Государственных образовательных стандартов (ГОС) высшего профессионального образования. Учтено, что требования ГОС ВПО по специальности "Бизнес-информатика" к освоению основных разделов дисциплины бакалаврами во многом идентичны аналогичным требованиям для других специальностей. Учитывая эту особенность, авторы попытались обобщить эти требования и предложить свою методику выполнения лабораторных занятий с учетом анализа мнений других ученых и преподавателей вузов, приведенных в списке литературы к данной работе.

Практикум является приложением к учебникам и лекционным курсам по информационной безопасности. Он предназначен для проведения лабораторных занятий и самостоятельной работы студентов по этой дисциплине. В нем рассмотрены практические основы проектирования и использования систем защиты информации (СЗИ), приемы работы пользователя с данными и информацией, аппаратно-программными и инженерно-техническими комплексами в защищенных компьютерных системах. Выполнение совокупности предложенных в практикуме сквозных практических заданий и подготовка ответов на контрольные вопросы обеспечит высокую эффективность обучения студентов работе на ПК.

По каждой из специальностей ФГОУ ВПО КубГАУ преподаватель, ведущий дисциплину "Информационная безопасность" самостоятельно выбирает (см. планы лекций и ПЗ /ЛЗ/ в приложении 1):

- тематику лабораторных занятий;
- их количество и
- объем самостоятельной работы студентов по дисциплине.

Студенты имеют возможности выполнять все задания практикума самостоятельно или под руководством и контролем преподавателя. Авторы понимают, что приведенная обобщенная структура дисциплины, названия разделов, темы лекций и лабораторных занятий отражает лишь основные разделы дисциплины. Поэтому, для полного освоения изучаемой дисциплины необходимо пользоваться указанной литературой и выполнить как можно больше заданий практикума. Работа позволяет получить общее представление об объеме дисциплины "Информационная безопасность и защита информации", а также может быть использована в качестве справочного пособия.

Методические рекомендации руководителю по подготовке и проведению занятия

1. Личная подготовка преподавателя к проведению занятия.

Условно ее можно разделить на *общую* и *непосредственную* подготовку.

Первая включает в себя изучение руководящих документов, определяющих задачи, содержание и организацию в целом процесса обучения, а также того или иного предмета обучения. Подбор и изучение руководящих документов и материала по теме занятия позволяет преподавателю углубить и повысить общий кругозор, правильно определить цель и последовательность проведения предстоящего занятия, правильно применять рекомендации старших начальников.

Изучив общие положения организации и методики изучения данного предмета обучения, преподаватель начинает непосредственную подготовку к проведению занятия. Основная цель этого этапа - разработать замысел занятия. При выборе методических приемов, применяемых на занятии, следует учитывать содержание учебных вопросов, подготовленность обучаемых, материальное обеспечение и учебные цели занятия. Необходимо стремиться к тому, чтобы выбранные методы обучения и методические приемы обеспечивали студентам возможность овладения не только знаниями, навыками, но и умениями. При расчете учебного времени необходимо учитывать содержание учебных вопросов и цель занятия (чего хочет добиться обучающий от обучаемых: овладение только знаниями или же знаниями, навыками и умениями).

При подготовке преподавателя к занятию необходимо подобрать ряд примеров, на которых можно показать практическую необходимость и значение данного вопроса. К каждому занятию следует исключительно тщательно продумать вопросы, которые будут ставиться перед обучаемыми во вводной части занятия и в ходе его.

Затем преподаватель подбирает наглядные пособия, необходимые для занятия, и определяет технические средства, которые будут использоваться на занятии, при этом нужно не только продумать порядок их использования, но и практически изучить правила пользования ими.

В заключении личной подготовки к проведению занятия преподаватель определяет место проведения занятия и какое требуется материальное обеспечение.

В итоге личной подготовки преподаватель составляет план проведения занятия. Он является основным рабочим документом преподавателя и должен быть прост и удобен для пользования на занятии.

Заключительным этапом работы преподавателя является подготовка места и материального обеспечения занятия. Для этого необходимо лично заблаговременно проверить, чтобы оборудование места, где будет проходить занятие, соответствовало установленным требованиям; действующие стенды и аппаратура были исправны и действовали, средства изобразительной наглядности были поучительными, правильными и соответствовали содержанию учебных вопросов.

2. Порядок оценки студентов при проведении занятия.

В процессе занятия бакалавра оценивается по следующим параметрам:

- оценка за ответ на вопрос;
- оценка за добавления;
- оценка за конспект.

По результатам выставляется суммарная оценка за ответ.

3. Критерии оценки студента.

Результаты контроля ответа бакалавра на учебный вопрос определяются частными оценками "отлично", "хорошо", "удовлетворительно" и "неудовлетворительно".

Оценка "отлично" - выставляется, если студент методически грамотно изложил суть учебного вопроса, формулировки четкие и логически завершенные, выводы конкретные.

Оценка "хорошо" - выставляется, если студент правильно излагает суть учебного вопроса, но допускает отдельные неточности не принципиального характера, выводы в ответе не отличаются конкретностью.

Оценка "удовлетворительно" - выставляется, если бакалавр правильно знает предназначение и основы функционирования программного обеспечения, без неточностей принципиального характера.

Оценка "неудовлетворительно" - выставляется, если бакалавр не знает сути учебного вопроса, самостоятельно заявляет преподавателю о незнании или неподготовленности к ответу по данному вопросу, не обладает логикой инженерного мышления, а также в тех случаях, когда не выполнены условия на оценку "удовлетворительно".

4. Предложения преподавателя по совершенствованию содержания и методики проведения занятия:

Кратко подвести итог изложенного материала. Повторить тему, цели, учебные вопросы выносимые на занятие. Объявить оценки и отметить лучших бакалавров. Ответить на возникшие вопросы в ходе занятия. Дать рекомендации по самостоятельной работе для углубления, расширения и практического применения знаний по данной теме. Поставить перед обучаемыми необходимые задачи на подготовку к следующему занятию, ответить на вопросы, возникшие за время занятия. Закончить занятие.

ЛАБОРАТОРНЫЕ ЗАНЯТИЯ

I. Основные термины теории информационной безопасности

Контрольные вопросы по теме

1. Разъяснить основные понятия информационной безопасности: сигнал, данные, информация, знания, система защиты информации.
2. Объект и предмет информационной безопасности.
3. Классификации АИС.
4. Каковы цели, задачи и содержание информатики?
5. Системы искусственного интеллекта.
6. Что такое системы поддержки принятия решений?
7. Сходство и различие понятий: данные и информатика.
8. Каковы основные свойства и формы представления информации?
9. Что такое кодирование данных?
10. Каковы основные структуры данных?

ЛЗ-01. Разработка модели разграничения доступа к информации

Цель: научить студентов разрабатывать модель системы защиты информации (СЗИ) от несанкционированного доступа (НСД) для автоматизированной системы (АС) конкретного объекта на основе изучения влияния организационной и информационной структур систем управления (СУ) «своего» объекта на информационную архитектуру его АС и на состав требований по защите информации от НСД. Студенты должны разработать модель информационной архитектуры самой АС в соответствии с параметрами СУ, которые указаны в вариантах индивидуального задания, определить класс защищенности АС, соответствующие ему требования по безопасности и разработать «свою» модель СЗИ от НСД для АС объекта.

Учебные вопросы:

- 1.1. Разработать перечень защищаемых ресурсов и их критичности.
- 1.2. Определить категории персонала и программно-аппаратных средств, на которые распространяется политика информационной безопасности.
- 1.3. Установить особенностей расположения, функционирования и построения средств компьютерной системы (КС) и выявить угрозы безопасности информации и класса защищенности АС.
- 1.4. Сформировать требования к построению СЗИ.
- 1.5. Определить места уязвимости АС и выбрать средства защиты информации.

Литература:

1. Гайкович В., Першин А. Безопасность электронных банковских систем. - М.: Единая Европа, 1994.
2. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. - М.: МИФИ, 1995.
3. Зегжда П.Д. и др. Теория и практика обеспечения информационной безопасности. – М.: Изд-во Яхтсмен, 1996. - 192с.
4. Медведовский И., Семьянов П., Платонов В. Атака через «INTERNET».- СПб: НПО «Мир и семья - 95», 1997.
5. Мельников В.В. Защита информации в компьютерных системах. - М.: Финансы и статистика, Электронинформ, 1997.
6. Галатенко В. Информационная безопасность//Открытые системы, № 4-6, 1995, № 1- 4, 1996.
7. Сборник руководящих документов по защите информации от несанкционированного доступа. – М: Гостехкомиссия, 1998. – 120 с.

8. Концепция национальной безопасности РФ. - сайт Правительства РФ, www.gov.ru.
9. Доктрина информационной безопасности РФ. - сайт Правительства РФ, www.gov.ru.

Учебно-материальное обеспечение:

1. Данные методические рекомендации и раздаточный материал к ним.

ВВЕДЕНИЕ

Разработка модели разграничения доступа к информации является одним из этапов проектирования СЗИ от НСД для защищенной АС объекта. СЗИ предназначена для автоматизации информационных процессов в системе управления (СУ) объектом, с целью повышения ее эффективности при решении функциональных задач.

На этапе разработки модели разграничения доступа к информации при создании СЗИ от НСД должна быть сформулирована политика информационной безопасности и разработан проект защищенной информационной архитектуры АС, которая должна поддерживать эту политику безопасности и быть согласованной с информационной архитектурой СУ по задачам обработки и защиты данных.

Под **политикой информационной безопасности** (далее политикой безопасности) автоматизированного участка СУ понимается совокупность принципов, правил, и практических рекомендаций, на основе которых строится управление, защита и распределение защищаемой информации в конкретной АС, зафиксированных документально.

Под **автоматизированной системой военного назначения (АС)** будем пониматься организационно-техническую структуру, представляющую собой совокупность взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи); методов и алгоритмов обработки данных в виде соответствующего программного обеспечения; информации (массивов, наборов, банков данных) на различных носителях; личного состава, в т.ч. должностных лиц - пользователей системы, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации (данных) с целью решения задач управления войсками и оружием.

Под **информационной архитектурой** понимается организационно-техническая структура системы управления, которая отражает логику взаимодействия элементов информационной системы в ходе обработки данных при решении функциональных задач.

Информационная архитектура может быть представлена набором функциональных схем, таблиц и других документов, содержащих следующую информацию:

- состав подразделений и должностных лиц, в чьих интересах будет функционировать информационная система (отделов и служб), а также подразделений и должностных лиц информационных служб (подразделений связи и автоматизации и т.п.), предназначенных для реализации функций обработки информации, с указанием функциональных обязанностей, необходимости и порядка взаимодействия при решении задач управления;
- перечни функциональных задач и задач по обработке информации, которые предполагается решать в системе с указанием их характеристик;
- перечень информационных массивов, наборов и банков данных, которые необходимо формировать и поддерживать в ходе решения функциональных задач и задач по обработке информации, с указанием носителей информации, предназначенных для их хранения, и ответственных за их актуализацию должностных лиц;
- структура физической и логической топологии информационной системы с указанием планируемых информационных потоков между элементами СУ и каналов связи между ними;
- организационно-техническая структура (архитектура) автоматизированных участков СУ с указанием технических средства обработки и передачи данных, методов и алгоритмов обработки данных в виде пакетов общего и специального программного обеспечения;

- других характеристик системы и ее компонентов, способных оказать влияние на ход информационного процесса.

Порядок разработки модели разграничения доступа в АС зависит от стадии жизненного цикла, на которой находится СУ, существующего уровня автоматизации и степени изученности. Объективно существует три ситуации, в которых может приниматься решение на создание СЗИ от НСД и разработку модели разграничения доступа к информации:

1. Создается новая СУ. Планируется решение задач управления с обработкой информации ограниченного доступа. Предполагается комплексная автоматизация всей системы или автоматизация некоторых участков (сегментов) обработки данных. Необходимые исходные данные для создания СЗИ от НСД разрабатываются параллельно с проектированием АС.

2. СУ уже существует. Имеются задачи управления, решение которых требует обработки информации ограниченного доступа. Предполагается комплексная автоматизация всей системы или автоматизация некоторых участков (сегментов) обработки данных. Часть необходимых исходных данных для создания СЗИ от НСД формируется в результате обследования организационно-штатной и информационной структуры СУ. Другая часть формируется параллельно с разработкой проекта АС.

3. СУ уже существует и в ее интересах функционирует АС, которая автоматизирует обработку данных на некоторых участках (сегментах) или во всей системе. СУ планируется настроить на решение задач управления, обрабатывающих информацию ограниченного доступа. Необходимые исходные данные для создания СЗИ от НСД формируются в результате обследования организационно-штатной и информационной структуры СУ, информационной и организационно-технической архитектуры существующей АС.

Если система управления только проектируется, то имеется возможность включить требования по безопасности информации в проект системы и учитывать их при разработке структуры и выборе компонентов информационной архитектуры создаваемой АС. Кроме того, существует возможность влиять на функциональные требования к информационной системе (в т.ч. на организационно-штатную структуру СУ) для их коррекции с целью выполнения требований по безопасности. Например, можно решить вопрос с выделением штатных единиц для органов ОБИ, использовать СВТ с более высоким классом защиты, изменить предполагаемые маршруты прохождения потоков секретной информации и т.п.

Если СУ уже существует и требуется автоматизация информационных процессов, то организационно-штатная структура уже сложилась, должностные лица и подразделения имеют функциональные задачи и, в целом, функциональные требования к АС уже слабо управляемы. Необходимо проводить тщательное обследование информационной архитектуры СУ, выявить все функциональные задачи и информационные потоки между ними и разработать архитектуру АС в защищенном исполнении.

В случае создания СЗИ от НСД для уже функционирующей АС задачи по разработке модели разграничения доступа остаются те же, однако модификация архитектуры АС уже требует больших затрат. Поэтому создание СЗИ от НСД для существующей АС является сложной задачей из-за невозможности выполнить некоторые требования по безопасности и обеспечить требуемый класс защиты АС от НСД к информации.

В качестве общего задания на лабораторную работу №1 по дисциплине «Информационная безопасность» предлагается разработать проект системы программно-аппаратной защиты АС от НСД при наличии первой из рассмотренных ситуаций, когда необходимо автоматизацию и защиту информационных процессов в СУ проводить одновременно. Следовательно, при выполнении ЛЗ-01 ставится задача

- обследования информационной архитектуры СУ,
- выработки политики ИБ и модели разграничения доступа,
- создания проекта АС для решения задач управления в защищенном исполнении.

Основные этапы решения этой задачи и рассмотрены в лабораторной работе №1.

ОСНОВНАЯ ЧАСТЬ

1.1. Разработать перечень защищаемых ресурсов и их критичности.

1.1.1. Определение необходимости формирования политики безопасности

Системы управления относятся к классу критических систем управления, для которых безопасность информации является одним из основных критериев эффективности. Поэтому при автоматизации информационных процессов в таких системах необходимо иметь четко сформулированную на основе законодательных и нормативно-руководящих документов политику информационной безопасности, которая должна реализовывать принятую в государстве концепцию обеспечения информационной безопасности и защиты информации. На базе национальной политики информационной безопасности формируется политика безопасности для конкретной критической системы управления и ее технологических участков, в том числе автоматизированных. Политика безопасности АС должна быть отражена в организационно-распорядительных документах, разрабатываемых при принятии решения на создание системы, а также на этапах ее проектирования, ввода в эксплуатацию и функционирования.

Исходными данными для формулирования политики безопасности АС являются:

- законы, указы и другие государственные законодательные акты, регулирующие правовые отношения в области информационной безопасности;
- руководящие, нормативные и методические документы, регламентирующие вопросы обеспечения безопасности информации, которые разрабатываются федеральными и ведомственными органами, входящими в систему защиты государственной тайны];
- информационная архитектура конкретной СУ (формируется в ходе исследования организационно-штатной структуры существующей или создаваемой СУ с указанием подразделений, должностных лиц, выполняемых ими функциональных задач с классификацией их по грифам секретности и категориям (тематике) и т.д.);
- архитектура автоматизированного участка защищаемой СУ (формируется в ходе исследования состава и структуры существующей или в ходе проектирования создаваемой АС);
- варианты построения систем защиты информации (СЗИ) от НСД в АС;
- тактико-технические характеристики средств вычислительной техники (СВТ) и защиты информации.

Система защиты информации от НСД, которая создается для обеспечения безопасности информации в автоматизированных системах военного назначения, должна реализовать необходимые и достаточные требования по защите информации от НСД, изложенные в государственных нормативно-руководящих документах. Состав требований по защите информации от НСД для конкретной АС формируется с учетом организационно-штатной структуры военной системы управления, характеристик решаемых задач и обрабатываемых данных, условий расположения, режимов функционирования и архитектуры комплекса технических средств обработки информации, в том числе средств вычислительной техники.

Основой для построения СЗИ от НСД в АС является формальная модель политики ИБ, которая представляет собой взаимосвязанную совокупность следующих элементов:

- множество защищаемых ресурсов информационной системы $R=\{r_i\}$, $r_i=(id_i, gr_i)$, где id - идентификатор ресурса, gr - уровень безопасности;
- множество пользователей информационной системы $U=\{u_j\}$, $u_j=(id_j, ul_j)$, id - идентификатор пользователя, ul — уровень доступа;
- совокупность правил разграничения доступа пользователей к ресурсам информационной системы $M=R \times U$;
- совокупность правил поведения пользователей системы;

множество источников угроз безопасности информации и соответствующих им угроз $S=\{sk\}$, $sk=\{tl, pl, dl\}$, t - угроза безопасности, p - вероятность проявления угрозы, d - величина наносимого ущерба;

- множество механизмов защиты информации $M=\{mn,\}$, $mn=(fn, cn)$, fn - реализуемая функция, cn - стоимость реализации механизма;
- совокупность правил управления механизмами защиты и средствами их интеграции;
- совокупность оценок результатов применения механизмов защиты информации $Rt=S \times M$;
- множество мероприятий по поддержанию и восстановлению работоспособности информационной системы.

Упрощенную модель политики информационной безопасности можно сформировать в неформальном виде в результате выполнения комплекса мероприятий. Формулирование и разработка политики информационной безопасности проводится в два этапа.

На **первом этапе** высшими звеньями управления определяются общие требования к политике информационной безопасности. Соответствующие законодательные и исполнительные федеральные органы власти, а также высшие должностные лица заинтересованных ведомств и организаций определяют важность сведений, обрабатываемых в информационных системах, выделяют тематические разделы и информационные службы, которые нуждаются в особой защите с точки зрения обеспечения целостности, доступности и конфиденциальности информации. Решения принимаются на основе концепции национальной безопасности и доктрины информационной безопасности РФ [8, 9], национальных и ведомственных концепций защиты информации и законов, регулирующих правовые отношения в информационной сфере. Требования политики безопасности фиксируются в государственных и ведомственных системах нормативно-руководящих документов по защите информации.

В системе нормативно-руководящих документов РФ, определяющих порядок формирования политики информационной безопасности, до настоящего времени отсутствует методология предъявления требований по безопасности и оценки защищенности информации от НСД, которая охватывала бы все направления защиты, как при использовании автоматизированных, так и традиционных технологий обработки информации. Поэтому в РФ используется первичная система нормативно-руководящих документов по защите информации от НСД в АС, разработанная государственной технической комиссией (ГТК) [7]. Она включает в себя систему нормативно-руководящих документов по защите информации с использованием криптографических средств защиты, разработанная ФАПСИ, а также нормативно-руководящие документы, регулирующие некоторые направления защиты информации, например, организацию защиты информации при использовании автоматизированных и традиционных «бумажных» технологий обработки данных, защиту от ПЭМИН, организацию режима секретности и др.

На **втором этапе** построения модели ИБ объекта разрабатывается политика безопасности и, соответствующая, модель разграничения доступа для конкретной АС, которые определяются командирами и начальниками воинских объединений, соединений, частей и учреждений (далее воинских частей), в интересах которых будет функционировать АС, с привлечением специалистов органов обеспечения безопасности информации, и согласуется с подрядчиками на разработку и производство защищенной АС.

Под **органом обеспечения безопасности информации (ОБИ)** понимается специальное штатное подразделение (одно или несколько должностных лиц), создаваемое в установленном порядке на этапах ввода объектов ВТ или их отдельных элементов в эксплуатацию с соответствующим штатным расписанием. При невозможности создания штатных органов их функции должны возлагаться на других должностных лиц объекта ВТ.

Действие политики безопасности распространяется на **объект защиты (объект вычислительной техники)**, под которым здесь понимается автоматизированная информационная система военного назначения или ее относительно функционально независимая часть, включающая в себя объединенные каким-либо образом компоненты, выполняющие функции по автоматизированной обработке информации в интересах подразделений и предоставляющие информационные услуги различного характера должностным лицам – пользователям организации.

Под **пользователем** понимается должностное лицо организации, которое самостоятельно обрабатывает информацию на средствах ВТ или в чьих интересах производится ее автоматизированная обработка.

Специальная комиссия организации определяет необходимость формирования политики информационной безопасности, исходя из наличия задач, которые предполагается решать в АС, и которые нуждаются в защите с точки зрения требований нормативно-руководящих документов, относящих информационные ресурсы системы к государственной, служебной или другим видам тайн и/или к определенным категориям информации ограниченного доступа. К таким ресурсам может быть отнесена информация, включенная в перечень сведений, подлежащих засекречиванию в РФ, или информация, доступ к которой ограничен требованиями законов, наставлений, руководств и других руководящих документов (например, сведения по мобилизационной и боевой готовности, шифрам, кадрам и т.п.).

При наличии информации ограниченного доступа принимается решение на создание системы защиты информации от НСД и определяются подразделения организации, информация которых наиболее критична. Для информации ограниченного доступа определяются грифы секретности и категории (тематики), соответствующие их важности с точки зрения защиты. В то же время определяются наиболее важные направления обеспечения безопасности информации в разных подразделениях, т.е. выделяются информационные компоненты, которые являются более зависимыми от нарушения их целостности и/или доступности и/или конфиденциальности.

1.1.2. Классификация защищаемой информации

Классификация информации по грифам секретности и категориям производится на основании приказов, наставлений, руководств и других руководящих документов, определяющих ограничения на доступ к информации определенного грифа секретности или определенной тематики. Признаком для ограничения доступа к сведениям могут быть также функциональные обязанности должностных лиц. Например, при наличии электронного учета документов необходимо ограничивать полномочия должностных лиц к модификации записей журнала учета, разрешив только добавлять новые записи (строки) или заполнять отдельные графы, используемые при проводке документов, должностному лицу, ответственному за учет.

Исходными данными для проведения классификация информации являются:

- уровень звена управления, для которого проектируется АС (определяется первым символом в индивидуальном задании на курсовую работу);
- организационно-штатная структура СУ с перечнем должностных лиц и подразделений в интересах которых будет функционировать АС (в работе определяется студентом в соответствии с выбранным для автоматизации сегментом СУ на основании исходных данных индивидуального задания о типе автоматизированной системы (архитектуры), условий расположения, распределении полномочий пользователей и состава информационной базы создаваемой АС);
- функциональные задачи, которые предполагается решать в АС в интересах подразделений и должностных лиц (в работе определяется студентом на основании выбранной в предыдущем пункте организационно-штатной структуры СУ);
- архитектура АС (разрабатывается курсантом на основании всех предыдущих пунктов исходных данных).

В каждой АС отрабатываются общий Перечень защищаемых ресурсов и Перечни защищаемых ресурсов подразделений или отдельных объектов ВТ, входящих в состав АС в качестве относительно независимых функциональных компонентов.

Перечни разрабатываются в процессе анализа решаемых в интересах подразделений функциональных задач, состава автоматизированных рабочих мест, организуемых банков данных, возможностей и режимов использования программных средств, а также средств, обеспечивающих обмен информацией между объектами АС. В Перечнях защищаемых ресурсов указываются сведения о допуске к этим ресурсам соответствующих подразделений или должностных лиц организации. Составление Перечней защищаемых ресурсов осуществляется совместно

представителями подразделений, органов автоматизации, связи и обеспечения безопасности информации АС.

Перечни защищаемых ресурсов необходимо оформить в виде официального распорядительного документа с приложением к нему сводного перечня задач, которые планируется решать в АС. Этот документ должен быть утвержден вышестоящим начальником организации, для АС разрабатываемых централизованно, если АС создается для решения задач только в интересах организации. Примерная форма Перечня защищаемых ресурсов на ОВТ представлена в таблице 1.

Таблица 1. Перечень защищаемых ресурсов на объекте ВТ
ЛВС оперативного отдела (ОО) и отдела кадров(ОК)
(наименование объекта, тип ЭВМ)

№ п/п	Защищаемый ресурс			К ресурсу допущены
	Полное наименование	Условное наименование	Гриф секретности	
1	2	3	4	5
1	Ключевой набор данных	RNLM2	Сов. секретно	Специалист по ОБИ
2	Рабочее место пользователя ОО	APM1	Секретно	Пользователи отдела
3	Рабочее место начальника ОО	APM2	Сов. секретно	Начальник и зам. начальника отдела
4	Рабочее место пользователей ОК	APM3	Секретно	Пользователи отдела кадров
5	База данных справочной системы ОО	БДССОО	Секретно	Пользователи оперативного отдела
6	Задача «Расчет сил и средств для решения задачи»	РСС	Сов. секретно	Начальник и зам. начальника ОО
7	БД данных справочной системы ОК	БДССОК	Секретно	Пользователи отдела кадров
8	Файл с данными по наличию бланков учета	777.doc	Несекретно	Пользователи отдела кадров
9	Сервер ЛВС	C1	Сов. секретно	Администратор безопасности ЛВС
10	ОС Windows NT 4.0	ОС336790422	Несекретно	Администратор безопасности ЛВС
11	...			

1.2. Определить категории персонала и программно-аппаратных средств, на которые распространяется политика информационной безопасности.

1.2.1. Определение правил разграничения доступа к информации между различными категориями персонала

На основе анализа особенностей информационного обмена между подразделениями и штатного состава подразделений определяются:

- необходимость работы некоторых штатных категорий должностных лиц с различными информационными компонентами, содержащими защищаемую информацию;
- должностные лица, ответственные за поддержание актуальности различных разделов информационной базы;
- перечень типов операций с различными категориями документов (чтение, изменение, уничтожение, создание и т.п.) для отдельных категорий пользователей.

1.2.2. Определение категорий персонала, на которые распространяются требования политики ИБ. Определение отношения к пользователям, осуществляющим доступ к информационным ресурсам из внешней информационной среды

Часть пользователей организации может иметь свои штатные автоматизированные рабочие места (АРМ), другая часть может совместно использовать АРМ-ы коллективного пользования. Некоторым должностным лицам может предоставляться право доступа к информационным ресурсам из-за пределов АС, например, командованию части или должностным лицам штабов вышестоящих и подчиненных звеньев управления и т.п. Необходимо строго определить эти категории пользователей в виде именных списков работников подразделений с обоснованием необходимости отнесения к той или иной категории.

В целях регламентации использования различных технических средств, в том числе мобильных компьютеров, множительной аппаратуры, средств печати документов, средств связи,

необходимо определить порядок их использования, ответственных должностных лиц, отвечающих за безопасность информации при их использовании.

Результатом работы должны стать таблицы разграничения доступа (ТРД) категорий должностных лиц подразделений к информационным массивам:

- общим для всей организации;
- относящимся к отдельным подразделениям (отдельно по каждому подразделению).

Для обеспечения функционирования системы разграничения доступа к информации и техническим средствам вычислительного комплекса (ВК) ответственным человеком (подразделением) за обеспечение безопасности информации (ОБИ) разрабатывается таблица разграничения доступа (ТРД) к защищаемым ресурсам. Исходными данными для составления ТРД к защищаемым ресурсам являются утвержденные руководителем организации перечни защищаемых ресурсов, заявки начальников подразделений организации на должностных лиц, допущенных к работе с этими ресурсами, списки подразделений и должностных лиц, предоставляющих информационные службы, с их функциональными обязанностями и обязанностями по защите информации от НСД.

ТРД составляются администратором по ОБИ или локальным администратором по ОБИ выделенного участка АС (например, ответственным по ОБИ оперативного отдела, если имеется отдельная ПЭВМ или ЛВС отдела). Основанием для включения должностных лиц в ТРД и предоставления им определенных полномочий к информационным ресурсам с указанием типов разрешенных доступов являются заявки на должностных лиц отделов и служб организации, допущенных к защищаемым ресурсам объекта ВТ, которые утверждаются руководителем организации.

Заявки на должностных лиц отделов и служб организации, допущенных к защищаемым ресурсам объекта, могут иметь форму, приведенную в таблице 2. Возможно применение других разрешенных типов доступов. Количество и наименование граф 5-7 может меняться в зависимости от типов доступов к ресурсам, которые способна регулировать используемая система защиты информации от НСД.

Таблица 2. Разделение ресурсов в организации

№ п/п	Фамилия и инициалы должностного лица, допущенного к защищаемым ресурсам ОБТ	Защищаемые ресурсы				
		полное наименование ресурса	условное наименование ресурса	разрешенные виды доступа к ресурсу		
				чтение	запись	запуск
1	2	3	4	5	6	7
1	Иванов И.И.	Файл 777.doc	FC375	да	да	-
		Файл verba.exe	EC025	-	-	да
		Файл verba.txt	FC376	да	да	-
2	Сидоров С.С.	Файл verba.txt	FC376	да	-	-
		Файл verba.exe	EC025	-	-	да
3	...					

1.3. Установить особенностей расположения, функционирования и построения средств компьютерной системы (КС) и выявить угрозы безопасности информации и класса защищенности

АС.

Формирование набора требований по безопасности производится на основании РД ГТК [7], в которых указаны требования по безопасности для соответствующих классов АС и СВТ, а также информации, полученной при анализе или проектировании информационной архитектуры СУ и АС, которые определяют особенности расположения, функционирования и построения средств компьютерной системы.

1.3.1. Анализ информационной архитектуры системы

1.3.1.1. Определение информационных потребностей должностных лиц подразделений

Для формирования детальных требований к построению СЗИ необходимо выделить основные информационные задачи, решаемые должностными лицами различных подразделений, в том числе распределение обязанностей по обработке информации между конкретными должностными лицами подразделений, способы и форматы представления и хранения информационных массивов (отдельных документов).

Так же определяются места хранения информационных массивов, возможности совместного хранения информационных массивов различными подразделениями, способы и режимы обмена информацией между подразделениями и необходимость такого обмена.

1.3.1.2. Формирование (определение) перечня информационных услуг (информационных служб, функциональных компонент), предоставляемых ИС пользователям

Как правило, пользователи информационной системы нуждаются в определенных информационных услугах, которые представляются им в функциональном виде. Например, в качестве основных информационных услуг (служб) могут выступать система электронного документооборота части, система шифрования данных, система обмена графической информацией и т.п. Однако, чтобы основные службы могли функционировать, необходимо установить ряд вспомогательных служб. Имеются в виду серверы баз данных, почтовые серверы, сетевые сервисы, мониторы транзакций и т.д. Операционные системы и оборудование также можно отнести к вспомогательным сервисам. Предоставление некоторых вспомогательных служб может потребовать привлечения дополнительной совокупности услуг.

На этом этапе необходимо сформировать отображение основных информационных служб на вспомогательные службы (конкретные компоненты информационной системы).

Типовой набор вспомогательных служб:

- совместное хранение информации;
- совместная обработка информации;
- совместное использование устройств печати документов;
- электронная почта;
- удаленный доступ внешних пользователей к ресурсам системы;
- доступ к внешним информационным ресурсам (к информационным системам других воинских частей или невоенных организаций); и др.

1.3.1.3. Определение особенностей программно-аппаратной организации ИС, способов и средств связи самостоятельных компонент системы, каналов и средств реализации связи ИС с внешней информационной средой

В защите нуждаются все информационные службы и коммуникационные каналы между ними. Для определения перечня необходимых механизмов безопасности нужно разработать или проанализировать существующую программно-аппаратную реализацию всех серверов, рабочих мест, каналов связи информационной системы, а также других коммуникационных систем, особенно связанных с элементами информационной системы.

Результатом работы должна быть структурная схема информационной системы, на которой отображаются:

- основные серверы системы (если они есть), в том числе выделяются серверы, доступные извне, с указанием применяемых операционных систем;
- элементы системы, которые являются узлами связи различных компонент (сегментов) информационной системы;
- рабочие места, непосредственно связанные с выделенными для этого серверами, а также имеющие возможность организации связи с другими серверами, с указанием применяемых операционных систем;
- рабочие места или локальные сети, из которых возможно осуществление доступа к внешним информационным службам, с указанием средств, при помощи которых осуществляется доступ;

- реализация сетевых взаимодействий и особенности построения кабельной инфраструктуры.

1.3.1.4. Определение особенностей размещения основных систем и служб ИС, а также прокладки и использования кабельной системы, линий и каналов связи

Для исключения физического доступа посторонних лиц к элементам информационной системы необходимо проанализировать их размещение и возможности предотвращения или затруднения несанкционированного контакта с техническими средствами, в том числе:

- помещения, где располагаются основные серверы и рабочие места, на которых производится обработка наиболее важной информации, контролируемость подходов к ним, способы охраны, в том числе противопожарной, и сигнализации;
- размещение в помещениях технических средств, особенно там, где возможно появление посетителей, с точки зрения недоступности для визуального обзора посторонними лицами;
- построение и размещение кабельных систем с точки зрения возможности доступа к ним посторонних лиц или несанкционированного подключения дополнительных устройств, расположения посторонних кабелей, способы и средства контроля за целостностью кабелей;
- особенности реализации связи с удаленными подразделениями, если для этого используются каналы связи или передачи данных общего пользования, например, каналы городской телефонной сети.

1.3.1.5. Определение особенностей расположения и использования элементов систем коммуникаций и жизнеобеспечения, которые оказывают или могут оказывать влияние на процессы обработки информации или состояние безопасности информации

Для функционирования системы, особенно с точки зрения обеспечения целостности ресурсов и правильности их функционирования, важным является построение систем жизнеобеспечения, в том числе системы электропитания, пожаротушения и других.

Другой стороной систем жизнеобеспечения является их взаимосвязь с общедоступными системами и большая разнесенность по территории, что критично с точки зрения предотвращения утечки информации за счет электромагнитных наводок.

Результаты работы по этому разделу являются основой для формирования детальных описаний политики безопасности в виде правил разграничения доступа к ресурсам конкретных информационных служб, а также для выявления существующих угроз безопасности информации и выбора необходимых дополнительных механизмов безопасности.

1.3.2. Формулирование политики ИБ подразделений и информационных служб

Работы данного этапа выполняются отдельно для каждого функционального подразделения или информационной службы совместно руководителями подразделения, администраторами системы и специалистами службы безопасности.

1.3.2.1. Определение особенностей функционирования службы

Определение особенностей функционирования службы заключаются в уточнении:

- конфигурации применяемых аппаратных и программных средств;
- режимов функционирования, временных интервалов работы;
- распределения обязанностей между обслуживающим персоналом;
- интенсивности информационного обмена;
- перечня и характера связей с другими компонентами;
- зависимости от функционирования других компонент информационной системы;
- построения и надежности источников электропитания и других систем обеспечения.

1.3.2.2. Определение перечня ресурсов, относительно которых решаются задачи обеспечения целостности и конфиденциальности, а также доступности для легитимных пользователей

Если информационной основой организации является вычислительная сеть, то в число аппаратных активов следует включить компьютеры, периферийные устройства, внешние интер-

фейсы, кабельное хозяйство и сетевое оборудование.

К программным активам, вероятно, будут отнесены операционные системы (сетевая, серверные и клиентские), прикладное программное обеспечение, инструментальные средства, программы управления сетью и отдельными системами. Важно зафиксировать, в каких узлах сети хранится программное обеспечение и из каких узлов используется.

Третьим, и наиболее важным, видом активов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, а также способы доступа к ним. Все это важно для оценки последствий нарушений информационной безопасности.

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

Требования же к системе защиты информационной системы в целом (методам и средствам защиты) должны определяться, исходя из требований к защищенности различных типов информационных служб и с учетом особенностей конкретных технологий обработки и передачи информации (уязвимости).

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

Порядок определения требований к защищенности циркулирующей в системе информации состоит из следующих этапов:

- составляется общий перечень типов информационных элементов, циркулирующих в системе (документов, таблиц). Для этого с учетом предметной области системы массивы информации разделяются на типы по ее тематике, функциональному назначению, сходности технологии обработки и другим признакам;
- для каждого типа информационных элементов, выделенного в первом пункте, и каждого критического свойства информации (доступности, целостности, конфиденциальности) определяются (например, методом экспертных оценок):

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

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

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

Пример оценки требований к защищенности некоторого типа информационных ресурсов приведен в таблице 3.

Таблица 3. Защищенность информационных ресурсов организации

Элементы данных	Уровень ущерба по свойствам информации			
	Конфиденциальность	Целостность	Доступность	Защита от тиражирования
N_1	Нет	Средний	Средний	Нет
N_2	Высокий	Средний	Средний	Нет
N_m	Низкий	Низкий	Низкий	Нет
В итоге	Высокий	Средний	Средний	Нет

1.3.2.3. *Определение способов реализации правил разграничения доступа пользователей к информационным ресурсам*

На основе разработанной политики безопасности определяется модель разграничения доступа, которая будет являться базой формирования правил разграничения доступа и выбора конкретных средств защиты информации.

Руководящие документы Гостехкомиссии РФ определяют необходимость реализации избирательного (дискреционного) управления доступом для информационных систем начального уровня безопасности и применения мандатного (полномочного) управления доступом для систем высших уровней безопасности.

Выбор модели должен основываться на сформулированной политике безопасности и возможностях, предоставляемых выбранным способом построения информационной системы и применяемыми программно-аппаратными средствами.

Простейшим представлением модели для избирательного управления доступом является матрица доступа (таблица 4).

Таблица 4. Матрица доступа

Пользователи	Информационные элементы			Программы		
	b1	b2	b3	x1	x2	x3
A1	Чтение, запись	Чтение	—	—	Запись	Пересылка
A2	Чтение	Чтение, исполнение	Чтение, запись	Пересылка	—	—

В матрице конкретно определяются допустимые действия каждого пользователя (строка) к каждому ресурсу системы (столбец).

Для описания управления доступом в терминах мандатной модели каждому пользователю присваивается атрибут, называемый, например уровнем доступа (допуска), а каждому ресурсу - уровень важности (секретности). Разрешение на выполнение операции с ресурсом описывается в виде набора правил, который регулирует отношения между процессом и ресурсом (файлом). Процесс представляет собой программу, выполняемую от имени какого-либо пользователя.

Целью выбора модели управления доступом является выражение сути требований по безопасности к данной системе. Для этого модель должна обладать несколькими свойствами:

- быть адекватной моделируемой системе и не избыточной;
- быть простой и абстрактной, и поэтому несложной для понимания должностными лицами, которые ответственны за ее реализацию.

3.2.4. *Определение лиц, ответственных за ведение информационных массивов службы, а также возможностей их модификации другими пользователями*

Для детализации правил разграничения доступа необходимо определить поименный список пользователей относительно каждого защищаемого ресурса (рабочее место, программа, информационный массив, отдельный документ (файл)) с указанием возможных действий, выполняемых над ресурсом для каждого пользователя.

Главной задачей является определение лиц, ответственных за поддержание надлежащего состояния каждого конкретного ресурса (собственников ресурсов).

Результат работы можно представить в виде списков пользователей с разделением по категориям:

- администраторы системы;
- администраторы рабочих групп (подразделений);
- владельцы информационных ресурсов;
- операторы информационных служб;
- привилегированные пользователи;
- рядовые пользователи;
- внешние пользователи.

Для каждой категории необходимо определить максимальные полномочия по изменению конфигурации системы и обрабатываемой информации в соответствии с возможностями, предоставляемыми средствами информационной службы.

К таким полномочиям можно отнести, например, следующие:

- включение в систему новых устройств и программ;
- изменение режимов функционирования системы;
- включение новых пользователей;
- возможность работы с удаленных рабочих мест и др.

1.3.2.5. Формирование исчерпывающего набора правил разграничения доступа конкретных пользователей к объектам информационной службы

Для каждого сервера, относящегося к информационной системе, определяются поименные перечни пользователей, для которых будут созданы (или уже созданы) учетные записи с соответствующими атрибутами доступа к информации и дополнительными полномочиями.

В соответствии с выбранным способом управления доступом формируются детальные правила разграничения доступа для каждого сервера и информационной службы. Желательно сформировать единый подход к управлению доступом, по меньшей мере, в рамках одной информационной службы (функционального компонента), для упрощения работы каждого пользователя.

Описание правил выполняется на языке выбранной модели управления доступом.

Правилами разграничения доступа строго очерчивается круг возможностей, которые имеет каждый конкретный пользователь по отношению к доступному ему подмножеству ресурсов.

1.3.2.6. Формулирование и оформление в виде организационно-распорядительных документов правил работы с конкретными информационными службами

Для регламентации поведения пользователей на рабочих местах и организации работы администраторов должны быть разработаны типовые инструкции для каждого рабочего места (частные инструкции по ОБИ).

В инструкциях для администраторов информационных служб определяются основные положения политики безопасности применительно к данной службе и подходы к распределению полномочий пользователей.

В инструкциях для пользователей определяются правила работы в каждой информационной службе, а также действия в нестандартных и аварийных ситуациях.

Особенно детально должны быть расписаны правила работы пользователей, которые осуществляют связь с внешними информационными системами, а также в сегментах системы, в которые разрешен доступ внешних пользователей.

1.3.3. Определение класса защищенности АС

Для того чтобы сформировать набор требований по безопасности, которым должна отвечать АС, необходимо определить ее класс защищенности. Класс защищенности согласно руководящему документу ГТК «Классификация АС и требования по защите информации» определяется на основании:

- перечня защищаемых ресурсов АС и их уровней конфиденциальности;
- перечня лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- матрицы доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
- режимов обработки данных в АС.

При исследовании или проектировании информационной архитектуры системы необходимо определить:

- режимы обработки информации (коллективный или индивидуальный), т.е. порядок использования АРМ или одним или несколькими пользователями;
- полномочия пользователей по доступу к конкретным информационным ресурсам (файлам, каталогам, дискам) и штатным средствам АС (АРМ, серверам, внешним каналам связи и т.п.);
- уровни секретности и категории защищаемой информации.

Для обработки секретной информации разрешается использовать только АС категорий 3А, 2А, 1В, 1Б, 1А.

Если АС состоит из одной или нескольких автономных АРМ, каждая из которых предназначена для индивидуального использования одним из пользователей, который допущен ко всей информации, располагаемой на этом АРМ и информация имеет один уровень секретности (не важно какой!), то АС относится к классу 3А.

Если в АС пользователи имеют одинаковые права доступа (полномочия) ко всей информации, обрабатываемой в АС и имеющей различные уровни секретности, то система относится к классу защищенности 2А.

Если в АС при тех же прочих условиях, что и для класса 2А, не все пользователи имеют доступ ко всей информации в системе, то система относится к первой группе. При этом отнесение АС к определенному классу производится на основании наличия информации определенного уровня конфиденциальности, соответственно, для обработки информации «особой важности» предназначены системы с классом защиты 1А, для «совершенно секретной» – 1Б и «секретной» – 1В.

1.4. Сформировать требований к построению СЗИ.

Определение класса защищенности АС позволяет сформировать набор требований по безопасности, которые предъявляются к этому классу систем. Эти требования изложены в РД ГТК. Кроме того, на основе класса защищаемой АС выбираются средства вычислительной техники (СВТ), которые должны иметь соответствующие классы защищенности СВТ:

- для класса защищенности АС 1В используются СВТ не ниже 4 класса;
- для класса защищенности АС 1Б используются СВТ не ниже 3 класса;
- для класса защищенности АС 1А используются СВТ не ниже 2 класса.

Для классов защищенности АС 3А и 2А выбираются СВТ классов защищенности не ниже 4, 3, и 2 в зависимости от грифа секретности обрабатываемой информации, соответственно «секретной», «совершенно секретной» и «особой важности».

Полный набор требований по безопасности к АС называется **Заданием по безопасности**, выполнение которого должно дать определенные гарантии защищенности информации от НСД.

1.5. Определить места уязвимости АС и выбрать средства защиты информации.

Выделение угроз безопасности преследует цель ранжирования их по степени опасности для функционирования информационной системы в зависимости от возможного ущерба.

1.5.1. Выбор анализируемых компонент ИБ, в рамках которых возможно возникновение нарушений безопасности

На основе работ, выполненных при анализе информационной системы, получено достаточно информации, чтобы определить направления, на которых наиболее вероятно возникновение угроз безопасности информации. В зависимости от построения системы можно задать уровень детальности рассмотрения (уровни декомпозиции) на основе, например, следующих градаций:

- информационная система в целом;

- сегменты информационной системы и средства связи между ними;
- серверы информационных служб и используемые сетевые технологии;
- рабочие станции различного назначения и их конфигурации;
- межсегментные устройства;
- средства связи с удаленными корреспондентами.

1.5.2. Определение точек информационного контакта анализируемых компонент с внешней информационной средой, через которые возможны нарушения ИБ

На основе результатов предыдущей стадии работ определяются элементы системы, в которых возможен физический контакт с внешней информационной средой, который может явиться основой для проявления угроз безопасности. Иллюстрацией подобной операции может быть следующий рисунок.

Контролируемой зоной на данном рисунке будем называть территорию организации, на которой исключено или существенно затруднено пребывание посторонних лиц. Посторонние лица - лица, не имеющие хотя бы временного пропуска.

При реализации угрозы безопасности в точках контакта информационной системы с внешней средой возникает канал утечки информации или канал проникновения в информационную систему.

Утечка информации может происходить за счет:

- разглашения информации;
- разведки информации;
- несанкционированного доступа в информационную систему.

Существование канала утечки информации всегда приводит к нарушению конфиденциальности информации, тогда как канал проникновения в информационную систему в большинстве случаев приводит к нарушению целостности или доступности информации.

1.5.3. Формирование моделей источников угроз безопасности информации

Угрозы безопасности при самом поверхностном рассмотрении можно разделить на несколько категорий относительно следующих классификационных признаков:

По наличию нарушителя:

- естественные, связанные со стихийными явлениями или авариями обеспечивающих систем;
- искусственные, связанные с деятельностью людей.

По наличию умысла:

- случайные, когда умысел отсутствует;
- умышленные, в противоположном случае.

Для построения модели информационной безопасности наибольший интерес представляют угрозы, причиной которых является наличие нарушителя (или злоумышленника).

Нарушитель - это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Исследовав причины

нарушений, можно либо повлиять на сами эти причины (конечно если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

При разработке модели нарушителя определяются:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);
- ограничения и предположения о характере возможных действий нарушителей.

По отношению к АС нарушители могут быть внутренними (из числа личного состава системы) или внешними (посторонними лицами).

Всех нарушителей можно классифицировать следующим образом.

По уровню знаний об АС:

- знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами;
- обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;
- обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;
- знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

По уровню возможностей (используемым методам и средствам):

- применяющий чисто агентурные методы получения сведений;
- применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);
- использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;
- применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

По времени действия:

- в процессе функционирования АС (во время работы компонентов системы);
- в период не активности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т.п.);
- как в процессе функционирования АС, так и в период не активности компонентов системы.

По месту действия:

- без доступа на контролируемую территорию организации;
- с контролируемой территории без доступа в здания и сооружения;
- внутри помещений, но без доступа к техническим средствам АС;
- с рабочих мест конечных пользователей (операторов) АС;
- с доступом в зону данных (баз данных, архивов и т.п.);
- с доступом в зону управления средствами обеспечения безопасности АС.

Могут учитываться следующие ограничения и предположения о характере действий возможных нарушителей:

- работа по подбору кадров и специальные мероприятия затрудняют возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий по преодолению подсистемы защиты двух и более нарушителей;
- нарушитель, планируя попытки НСД, скрывает свои несанкционированные действия от других сотрудников/

НСД может быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки информации и т.д.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика. Каждый вид нарушителя должен быть охарактеризован значениями характеристик, приведенных выше.

1.5.3.1. Информационные каналы, выходящие за пределы предприятия

Информационные каналы можно подразделить на:

- Выделенные каналы (предназначенные для передачи особо секретной информации);
- Каналы, по которым передается конфиденциальная информация;
- Каналы, по которым передается несекретная информация.

Кроме того, можно разделить каналы связи, используемые для передачи информации, на общедоступные и принадлежащие ведомству или организации. Для организации информационных каналов первых двух видов предпочтительнее использовать ведомственные системы связи, так как для них легче организовать применение технических средств защиты и контроля их целостности. Каналы общего пользования подвержены как пассивным, так и активным угрозам, в то время как ведомственные каналы, как правило, недоступны для активного вмешательства, или такое вмешательство легко обнаруживается.

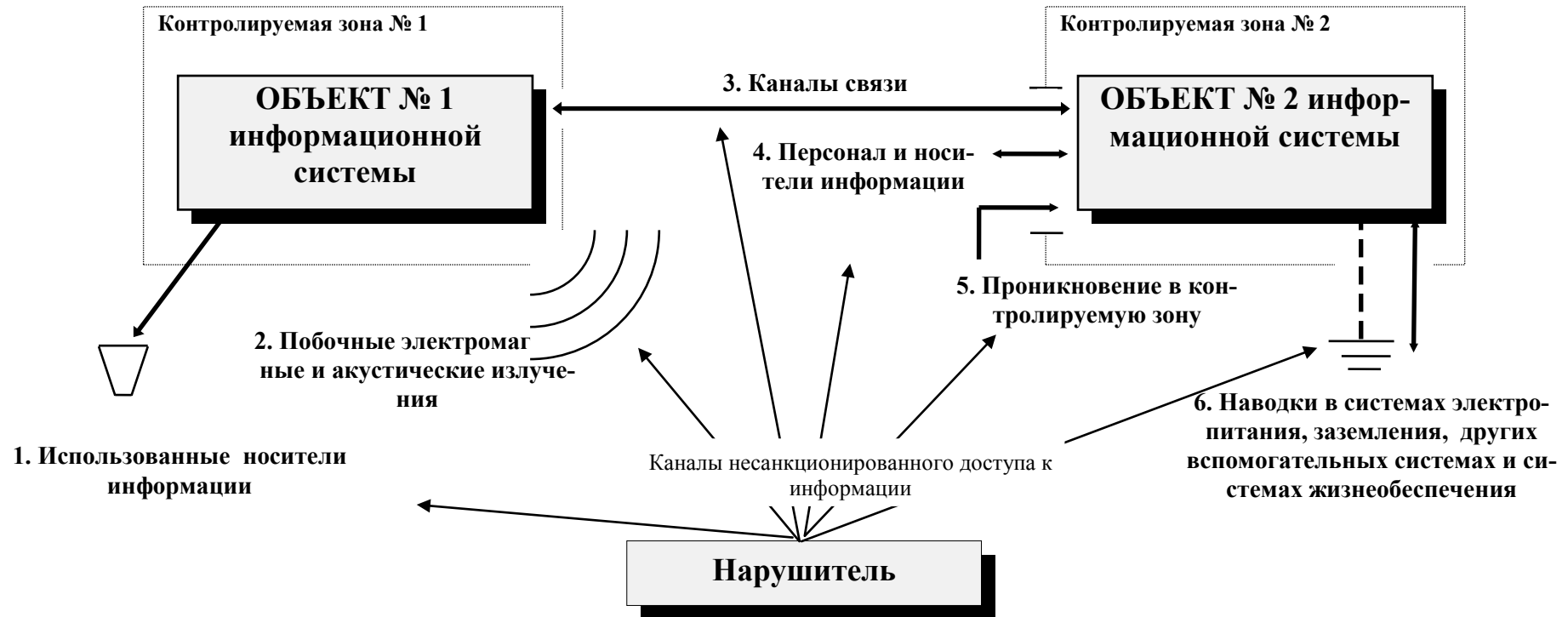
5.3.2. Побочные электромагнитные и другие излучения и наводки

Основные каналы утечки информации, возникающие за счет физических полей, можно проиллюстрировать следующей таблицей:

Таблица 4. Каналы утечки информации в АС

Каналы утечки информации	Виды перехватываемой информации
Акустический канал.	Речевые и прочие акустические сигналы.
Виброакустический канал.	Речевые и прочие акустические сигналы.
Утечка по проводному каналу (токонесущим инженерным коммуникациям).	Речевые и прочие акустические сигналы. Факсимильная, телеграфная, телетайпная информация. Информация, обрабатываемая на ЭВМ, или транслируемая по модемным каналам.
Электромагнитные поля.	Информация передаваемая по радиотелефону и радиосвязи. Информация передаваемая по радиомодему.
Побочные электромагнитные излучения и наводки.	Информация, обрабатываемая на ЭВМ. ПЭМИН вспомогательного оборудования, промоделированные полезным акустическим сигналом
Оптический.	Скрытая фото-, кино-, видеосъемка. Видеонаблюдение извне зоны охраны.

Данные каналы характеризуются их объективным существованием в пространстве, окружающем информационную систему. Практически не существует способов полного перекрытия данных каналов, однако выполнение мероприятий и применение специальных технических средств позволяет снизить вероятность проявления угрозы и существенно затруднить возможности злоумышленника по получению информации.



1.5.4. Выбор механизмов и средств защиты информации от НСД

1.5.4.1. Выбор защитных механизмов, предназначенных для предотвращения выявленных угроз ИБ или для усиления системы защиты, а также способов их реализации

Механизмы защиты информации являются достаточно специфичными и направленными на решение ограниченного круга задач безопасности. Поэтому необходимо сопоставить те свойства информации, которые предполагается обеспечивать в первую очередь, и возможные пути нарушения этих свойств. Результат такого сопоставления может быть представлен в виде таблицы 5.

Таблица 5. Средства защиты информации в АС

Способы нанесения ущерба	Объекты воздействий			
	Оборудование	Программы	Данные	Персонал
Раскрытие (утечка) информации	Хищение носителей информации, подключение к линии связи, несанкционированное использование ресурсов	Несанкционированное копирование перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашение, халатность
Потеря целостности информации	Подключение, модификация, спецвложения, изменение режимов работы, несанкционированное использование ресурсов	Внедрение “Троянских коней” и “жучков”	Искажение, модификация	Вербовка персонала, “маскарад”
Нарушение работоспособности автоматизированной системы	Изменение режимов функционирования, вывод из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение
Незаконное тиражирование (воспроизведение) информации	Изготовление аналогов без лицензий	Использование незаконных копий	Публикация без ведома авторов	

Для определения способов реализации механизмов защиты информации производится анализ возможности решения задач защиты информации из следующего перечня:

- введение избыточности элементов системы;
- резервирование элементов системы;
- регулирование доступа к элементам системы;
- защитное преобразование данных;
- контроль элементов системы;
- регулирование использования элементов системы;
- регистрация сведений об использовании элементов системы;
- уничтожение информации, потерявшей актуальность;
- сигнализация о попытках нарушения безопасности;
- реагирование на попытки нарушения безопасности.

Основу любой СЗИ составляет совокупность некоторых механизмов защиты информации, которые можно выделить на основе различных критериев. Обычно выделяют следующие механизмы (или службы безопасности):

- идентификацию и аутентификацию,
- управление доступом,
- протоколирование и аудит,
- криптографию,
- экранирование.

Выбор способа реализации механизмов защиты информации и решения задач защиты заключается в выборе типа средств, которые планируется использовать для решения каждого из механизмов:

- организационные;
- инженерно-технические (физические);
- программно-технические;

- криптографические.

1.5.4.2. Определение функциональных компонент (информационных служб), в которых предполагается использовать выбранные механизмы защиты

Реализация политики безопасности информации в разных компонентах системы, как правило, строится на основе разных подходов и преследует разные цели в соответствии с тем, что в разных информационных службах главный упор делается на разные свойства информации (целостность, доступность, конфиденциальность).

Реализация механизмов защиты информации базируется на двух подходах:

- использование встроенных в основные информационные службы (в том числе операционные системы, прикладные программы и др.) средств защиты;
- использование дополнительных экранирующих (навесных) средств защиты.

Задачей распределения механизмов защиты по компонентам является построение наиболее экономичной и наиболее эффективной системы защиты информации. Рациональным подходом в данном случае может рассматриваться использование одного механизма (или одного набора средств) для некоторой обслуживания некоторой совокупности взаимодействующих информационных служб.

Основное внимание уделяется недостатком используемых аппаратных и системных программных средств для определения необходимости применения в отдельных элементах информационной системы дополнительных средств защиты информации.

1.5.4.3. Определение способов интеграции механизмов безопасности в комплексную систему защиты информации (КСЗИ)

В настоящее время имеется большое количество разнообразных средств защиты информации, ориентированных на решение различных задач на основе различных вычислительных платформ.

Задача интеграции средств защиты информации стоит особенно остро, если АС создавалась длительное время из разнородных компонентов. При этом появляется более общая проблема интеграции самих компонент информационной системы.

В качестве подхода к интеграции средств защиты информации для разнородной информационной системы можно предложить выбор или построение средств защиты на основе однотипных сетевых технологий, что позволит организовать информационный обмен между элементами комплексной системы защиты и построить основу для создания централизованной системы управления защитой информации.

Дополнительным основанием для объединения средств защиты может служить соответствие их общепринятым международным (или государственным) стандартам, также производство их одной организацией.

При организации работ в разнородных информационных системах необходимо обращать внимание на достижение непротиворечивости реализации политики безопасности в разных компонентах системы, а также полноты реализации функций защиты информации в информационной системе в целом.

Для построения АС должны выбираться только сертифицированные СВТ и криптографические средства защиты информации. Перечни сертифицированных СВТ и криптографические средства защиты информации публикуются подразделениями Гостехкомиссии РФ и ФАПСИ.

1.5.4.4. Оценка остаточного риска

После определения конфигурации системы защиты информации необходимо заново оценить оставшиеся угрозы безопасности информации в соответствии с изменившимися параметрами информационной системы. Оценив новые параметры угроз, необходимо принять решение о применении дополнительных средств защиты информации или о достижении требуемого уровня безопасности информационной системы.

1.5.4.5. Определение способов реагирования на нарушения ИБ и планирование восстановления работоспособности после нарушений безопасности ресурсов ИС

Комплексная система защиты должна предусматривать необходимые средства сигнализации о попытках нарушения безопасности информационной системы, блокирования нарушителей в ходе реализации угроз безопасности, а также содержать подробный план действий при возникновении аварийных ситуаций с назначением ответственных лиц за каждый участок работы.

Для быстрого восстановления работоспособности информационных служб важную роль играют средства создания и хранения архивных копий информации, а также соответствующим образом разработанная стратегия архивирования.

ЗАКЛЮЧЕНИЕ

Модель информационной безопасности и модель разграничения доступа к информации служат основой проектирования комплексной системы защиты информации, а также разработки методик контроля защищенности информационной системы.

Построение модели разграничения доступа адекватной угрозам информации позволяет создавать защищенные АС с определенным уровнем безопасности.

Кратко подвести итог изложенного материала. Повторить тему, цели, учебные вопросы выносимые на занятие. Объявить оценки и отметить лучших студентов. Ответить на возникшие вопросы в ходе занятия. Дать рекомендации по самостоятельной работе для углубления, расширения и практического применения знаний по данной теме. Поставить перед обучаемыми необходимые задачи на подготовку к следующему занятию, ответить на вопросы, возникшие за время занятия. Закончить занятие.

ПРИЛОЖЕНИЯ К ЛЗ-01:

Приложение 1.1.

1. Таблица распределения вариантов значения исходных данных по вариантам заданий

Варианты значений исходных данных	Номер варианта индивидуального задания																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Общая структура системы управления																					
- несколько структурных подразделений в одном здании	+			+			+			+				+			+		+		
- несколько структурных подразделений в близко - расположенных зданиях		+			+			+			+				+			+		+	
- несколько территориально разнесенных зданий			+			+			+			+				+			+		+
Характер информационной деятельности																					
- орган государственного управления	+	+	+										+	+	+						
- государственная организация				+	+	+										+	+	+			
- кредитно-финансовое учреждение							+	+	+										+	+	+
- коммерческое предприятие										+	+	+									
Уровень конфиденциальности информации																					
- общедоступная информация			+		+		+		+		+				+				+		+
- персональные данные	+	+			+	+			+	+			+	+			+	+			+
- сведения, составляющие коммерческую, банковскую или служебную тайну	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
- секретные сведения	+		+	+	+						+		+	+	+		+	+	+		+
- совершенно секретные сведения				+	+									+			+	+			
- сведения особой важности				+													+				
Распределение полномочий пользователей																					
- пользователи имеют одинаковые права доступа к информации																					
- пользователи имеют разные права доступа к информации																					
Особенности первичной сети связи																					
- коммутируемые каналы телефонной сети общего пользования	+	+	+		+	+		+	+	+	+	+		+	+	+	+		+	+	
- выделенные каналы ТЧ		+		+	+		+			+		+	+			+			+		+

- выделенные цифровые каналы			+					+			+				+			+		
Реализуемые информационные ресурсы																				
- обмен данных	+	+	+	+	+	+		+	+	+	+	+		+	+	+	+		+	+
- доступ в ИВС ОП		+	+	+		+	+	+	+	+		+	+	+	+		+		+	+
- электронная почта	+		+		+		+		+		+		+		+		+		+	+
- вывод документов на печать																				
- доступ в базы данных	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
- электронный документооборот	+		+	+	+	+		+	+	+		+	+	+	+	+	+			+
- передача голосовых сообщений	+	+		+	+		+				+	+		+		+		+	+	+
- передача видеоизображения		+				+					+				+			+	+	

Приложение 1.1.

2. Таблица закрепления вариантов индивидуальных заданий за студентами учебной группы

№ п/п	Номер варианта индивидуального задания	Фамилия и инициалы руководителя	Фамилия и инициалы исполнителя	Подпись исполнителя в получении задания
1	2	3	4	5
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				

II. Общая характеристика процессов сбора, обработки и накопления информации

Контрольные вопросы по теме

1. Что из себя представляет процесс восприятия информации?
2. Дать определение сигнала и процесса его обработки.
3. Каковы уровни зрительного восприятия информации?
4. Состав современной системы сбора информации.
5. Как организуется процесс передачи информации?
6. Обработка информации и ее режимы.

ЛЗ-02 Разграничение доступа к информации в ОС Windows

Контрольные вопросы

Цель: Изучить и практически опробовать основные принципы обеспечения ЗИ в АС, использующей среду ОС Windows. Студенты уясняют и выполняют задания ЛЗ и выполняют все работы по ним.

Учебные вопросы:

- 2.1. Создание учетных записей пользователей.
- 2.2. Создание учетных записей групп.
- 2.3. Организация общего доступа к папкам
- 2.4. Защита сетевых ресурсов средствами файловой системы

Литература

1. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. - М.: МИФИ, 1995.
2. Зегжда П.Д. и др. Теория и практика обеспечения информационной безопасности. – М.: Изд-во Яхтсмен, 1996. - 192с.
3. Медведовский И., Семьянов П., Платонов В. Атака через «INTERNET».- СПб: НПО «Мир и семья - 95», 1997.
4. Мельников В.В. Защита информации в компьютерных системах. - М.: Финансы и статистика, Электронинформ, 1997.
5. Галатенко В. Информационная безопасность//Открытые системы, № 4-6, 1995, № 1- 4, 1996.

2.1. Создание учетных записей пользователей

Чтобы и далее упростить процесс управления пользователями, Microsoft предусмотрительно создает встроенные группы (как локальные, так и глобальные). Обратите внимание - встроенные группы нельзя удалить или переименовать /2/. Обычно эти группы оказываются удобными для администрирования прав и ограничений пользователей. Кроме того, некоторые пользователи включаются в эти встроенные группы по умолчанию. Пользователей можно включать или удалять из этих групп по своему усмотрению.

Работа с User Manager For Domains

User Manager For Domains — основной инструмент для управления правами пользователей. Ниже перечислены основные функции и задачи User Manager For Domains:

- Создание, изменение, дублирование и удаление групповых учетных записей.
- Создание, изменение, дублирование и удаление учетных записей пользователей.
- Установка политики учетных записей (выбор стандартных требований к паролям, параметров блокировки учетных записей, статуса отключения и т. д.).
- Создание прав и определение политики аудита для пользователей.
- Установление доверительных отношений.

Создание новых пользователей и групп

В большинстве сетей управление на уровне отдельных пользователей связано с множеством затруднений. Для упрощения задач администрирования сетевая Windows содержит специальную программу - User Manager For Domains (вызывается из меню Start - Start > Programs > Administrative Tools (Common) > User Manager For Domains). В User Manager For Domains администраторы создают учетные записи пользователей и групп, а также работают с ними. Когда вы освоитесь с этой программой, User Manager For Domains станет вашим основным инструментом для управления доступом на уровне пользователей и групп.

Для упрощения работы (и экономии вашего времени) управление пользователями основано на концепции группового администрирования. Вместо того чтобы заниматься отдельными пользователями, намного удобнее распределить их по группам и назначать права сразу для целой группы. Как только пользователь включается в группу, он наследует все права и ограничения доступа, присвоенные данной группе.

Чтобы создать в User Manager For Domains новую учетную запись пользователя или группы, выполните следующие действия:

1. Запустите User Manager For Domains и откройте меню User.
2. Выберите команду New User для создания пользователя (или команду New Group для создания группы).
3. Заполните диалоговое окно New User: введите имя пользователя (User Name), полное имя (Full Name) (необязательно), описание (Description) (необязательно), пароль (Password) и подтверждение пароля (Confirm Password).
4. Установите соответствующие флажки в нижней части окна New User, если:
 - Пользователь должен изменить пароль при первом входе в систему.
 - Пользователю не разрешается менять свой пароль.
 - Для пароля не существует ограничений срока действия.
 - Учетная запись отключается.

Кроме четырех флажков в нижней части диалогового окна находятся шесть кнопок. Они управляют многими возможностями, доступными для данного пользователя:

- Groups (Группы). Кнопка позволяет добавить пользователей в группу (или группы) или удалить их.
- Profiles (Профиль). Кнопка позволяет определить путь к профилям конкретного пользователя, к сценариям входа и основному каталогу пользователя.
- Hours (Время). Кнопка позволяет задать интервал времени, в течение которого пользователю разрешается вход в сеть. Если к концу разрешенного времени пользователь уже зарегистрирован, то по умолчанию он остается в сети, однако повторный вход станет возможным лишь с наступлением разрешенного интервала. Вы также можете установить принудительное отключение пользователя в определенное время, это делается с помощью политики учетной записи пользователя (см. далее).
- Logon To (Вход с). Кнопка разрешает вход пользователя в систему только с определенных компьютеров. Тем не менее, пользователи редко остаются на одном месте, поэтому желательно оставить значение по умолчанию (вход с любой рабочей станции).
- Account (Учетная запись). Здесь задается срок окончания действия учетной записи (полезно для временных или контрактных работников). По умолчанию используется значение Never (Никогда), однако вы можете ввести определенную дату. Кроме того, учетную запись можно сделать локальной (для пользователей из доменов, для которых не установлены доверительные отношения) или глобальной (для учетных записей обычных пользователей в домене).
- Dialin (Связь). Здесь пользователю предоставляется возможность модемного подключения к сети, а при необходимости задается такой элемент защиты, как ответный звонок сервера.

Модификация существующих учетных записей

Создание учетных записей пользователей является одной из самых распространенных задач сетевых администраторов. Новые пользователи часто занимают место уже существующих - переименовать учетную запись работника, переведенного на другое место, проще, чем созда-

вать новую. Для этого достаточно выполнить команду User > Rename в User Manager For Domains. Не забудьте предупредить нового работника о том, чтобы он сменил пароль при первом входе, потому что среди прочих параметров будет сохранен и старый пароль.

К сожалению, учетные записи пользователей довольно часто удаляются случайно. Единственный выход из положения - заново создать учетную запись с тем же именем, правами и ограничениями. Сделать это проще, чем кажется, потому что вы можете создать шаблоны прав пользователей для отделов и групп. Затем из меню User вы копируете шаблон, переименовываете его для нового пользователя и продолжаете действовать с этой точки, если вам потребуется задать дополнительные права или ограничения.

Если для пользователя были изменены права доступа, этот пользователь должен завершить работу и войти заново - лишь тогда новые права вступят в силу.

Задание:

1. Войти в систему под именем, выданным администратором.
2. Проверить учетную запись и ее возможности с помощью описанных выше команд.
3. Зарегистрировать три пользователя с учетными записями user1, user2, user3.
4. Проверить учетные записи и их возможности с помощью описанных выше команд.

2.2. Создание учетных записей групп

Без группового администрирования управление пользователями было бы довольно сложной задачей. Основная идея - присваивать права доступа только группам, а затем управлять правами отдельных пользователей, включая или удаляя их из различных групп по мере необходимости. Если следовать этому принципу, вам почти не придется задавать права доступа к ресурсам для отдельных пользователей. Учетным записям пользователей практически не назначают никакие права - все они наследуются от групп, к которым принадлежат пользователи.

Хороший подход к реализации безопасности пользователей в сетевой Windows заключается в том, чтобы создать группу для каждого ресурса в сети. Для каждого ресурса будет существовать группа, управляющая доступом к нему. После создания таких групп вам придется в основном управлять группами и их членами, а не конкретными ресурсами.

В сетевой Windows существует два вида групп: локальные и глобальные. Локальные группы доступны лишь в локальном домене; глобальные группы распространяются за пределы доменов. Вы должны хорошо понимать это принципиальное отличие. Другое важное отличие заключается в том, что локальные группы могут содержать и пользователей, и другие группы, тогда как глобальные группы содержат только пользователей. Никакие локальные или глобальные группы не могут входить в другую глобальную группу.

Итак, если вы хотите предоставить домену Engineering доступ к цветному принтеру в домене Marketing, следует создать глобальную группу (например, EngnrPrint) и разрешить ей доступ к принтеру. Снова обратите внимание: тот факт, что домен Marketing доверяет глобальной группе EngnrPrint доступ к цветному принтеру, вовсе не означает, что один домен обладает какими-либо дополнительными правами для ресурсов другого домена, если такие права не были специально заданы.

Как упоминалось выше, в сетевой Windows существует несколько встроенных локальных и глобальных групп, которым по умолчанию назначаются определенные привилегии. В табл. 2.1 перечислены эти группы (локальные и глобальные) вместе со стандартными членами и описаниями.

Кроме того, каждая группа обладает определенным типом доступа на уровне каталогов:

- Full Control (Полный доступ) — пользователи могут добавлять, читать и изменять файлы, изменять разрешения для каталогов и становиться владельцами каталогов и файлов.

Таблица 2.1. Встроенные группы в сетевой Windows

Название группы	Стандартные члены	Локальная/глобальная	Описание
Account Operators (операторы учетных записей)	Нет	Локальная	Члены группы могут администрировать учетные записи пользователей

			и групп
Administrators (администраторы)	Администраторы домена, Администратор	Локальная	Члены группы обладают неограниченными возможностями администрирования компьютер/домен
Backup Operators (операторы архива)	Нет	Локальная	Члены группы имеют доступ с целью архивации файлов
Domain Admins (администраторы домена)	Администратор	Глобальная	Назначенные администраторы домена
Domain Guests (гости домена)	Гость	Глобальная	Все гости домена
Domain Users (пользователи домена)	Администратор	Глобальная	Все пользователи домена
Guests (гости)	Гость	Локальная	Пользователи, которым был предоставлен доступ к компьютеру/домену
Everyone (Все)	Все	Глобальная/ локальная	Все пользователи
Print Operators (операторы печати)	Нет	Локальная	Члены группы могут администрировать принтеры домена
Replicators (репликаторы)	Нет	Локальная	Поддержка репликации файлов в домене
Server Operators (операторы сервера)	Администратор	Локальная	Члены группы могут администрировать серверы домена
Users(пользователи)	Пользователи домена	Локальная	Обычные пользователи

- List (Право просмотра) — пользователи могут получать списки файлов и подкаталогов данного каталога.

- Read (Право чтения) — пользователи могут читать файлы и запускать приложения из каталога.

- Add (Право добавления) — пользователи могут добавить в каталог новые файлы, но не могут изменить их.

- Add & Read (Право добавления и чтения) — пользователи могут добавлять и читать файлы в каталоге, но не могут их изменять.

- Change (Право изменения) — пользователи могут добавлять, читать и изменять содержимое файлов каталога.

- No Access (Нет доступа) — пользователи не могут обратиться к каталогу (даже если они являются членами других групп, которым такой доступ разрешен).

Совет

Когда пользователь принадлежит нескольким группам домена, приоритетным является право с минимальными ограничениями. Например, если пользователь имеет полный доступ для одной группы и право чтения — для другой, то в результате он будет иметь привилегии полного доступа. Кстати говоря, отсутствие доступа означает ПОЛНОЕ ОТСУТСТВИЕ ДОСТУПА!

Задание: Создать локальные группы Group12, содержащую первого и второго пользователя, и Group23, куда будут входить пользователи user2 и user3 соответственно.

2.3. Организация общего доступа к папкам

Стандартный подход к совместному использованию файлов, каталогов и ресурсов на компьютерах с сетевой ОС Windows заключается в создании общих имен. Чтобы организовать общий доступ к ресурсу или каталогу, выполните следующие несложные действия:

1. Выделите нужный каталог или ресурс в Explorer или с помощью значка My Computer.

2. Щелкните правой кнопкой мыши на каталоге или ресурсе и выберите из контекстного меню команду Sharing (по умолчанию выбрана строка Not Shared).

3. Нажмите кнопку Share As. При этом на экране появляется диалоговое окно, в котором сетевая Windows выводит общее имя по умолчанию (обычно оно совпадает с начальными буквами символами выделенного каталога). При желании вы можете изменить общее имя. Тем не менее помните о том, что общие имена, длина которых превышает восемь символов, будут недоступны из DOS-клиентов.

На вкладке Sharing можно ограничить доступ к ресурсу, указывая максимальное количество пользователей. Ограничение количества пользователей позволяет избежать перегрузки медленного компьютера или обеспечить нормальную работу всех остальных серверных процессов. Если подобные ограничения не нужны, установите переключатель Maximum Allowed. Чтобы установить максимальное количество пользователей, установите переключатель Allow, и в поле Users появится некоторое число. Вы можете увеличить или уменьшить это число с помощью кнопок со стрелками или же ввести число непосредственно в поле Users.

Внимание! По умолчанию подкаталоги наследуют права доступа своих родительских каталогов.

После того как общее имя будет создано, для него можно назначить необходимые разрешения. Для этого нажмите кнопку Permissions или щелкните на вкладке Security. Обратите внимание — по умолчанию для вновь создаваемых имен всем предоставляется право полного доступа (Full Control). Существует четыре степени безопасности, ограничивающие доступ к общим ресурсам сервера: отсутствие доступа (No Access), право чтения (Read), право изменения (Change) и полный доступ (Full Control).

Совет

Всегда явно задавайте разрешения доступа для всех создаваемых общих имен. По умолчанию группе Everyone предоставляется полный доступ!

Для контроля над доступом к общим ресурсам также можно воспользоваться программой Server Manager:

1. Запустите Server Manager (Start >• Programs >• Administrative Tools (Common) >• Server Manager).

2. Выделите нужный компьютер и выполните команду Properties из меню Computer.

3. Установите один из следующих переключателей:

- Users (Пользователи) — переключатель выводит количество пользователей, подключенных к ресурсу.

- Shares (Общие имена) — переключатель выводит все общие имена для домена, количество пользователей, работающих с общими ресурсами, и локальное имя общего ресурса.

- In Use (Используемые ресурсы) — переключатель выводит данные обо всех открытых ресурсах домена; пользователях, открывших ресурсы; типе операций, выполняемых с ресурсами; количестве блокировок для ресурсов и пути к открытым ресурсам.

- Alerts (Сигналы) — переключатель позволяет построить список всех компьютеров в сети, получающих административные сигналы.

Чтобы создать общее имя в Server Manager, выполните следующие действия:

1. Запустите Server Manager.

2. Выделите имя компьютера, на котором будет создано общее имя.

3. Выполните команду Shared Directories из меню Computer.

4. Нажмите кнопку New Share, введите имя и путь к общему ресурсу и нажмите кнопку ОК.

Внимание ! Для управления общими ресурсами в удаленном режиме пользуйтесь программой Server Manager, а не Windows Explorer.

Существует ряд административных общих ресурсов, скрытых от пользователей, но доступных для администратора. Имена этих общих ресурсов заканчиваются знаком доллара (\$), благодаря чему они остаются скрытыми. В табл. 2.2 перечислены эти общие ресурсы и приведены их описания.

Внимание! Встроенные административные ресурсы сетевой Windows невозможно удалить или переименовать.

Таблица. 2.2. Скрытые административные общие ресурсы сетевой Windows

Имя общего ресурса	Описание
Admin\$	Каталог, в котором установлен Windows Server (или Workstation), и каталог, используемый для удаленного администрирования сетевой Windows

Driveletter\$	Буква диска, на котором установлен носитель информации. Может использоваться в удаленном режиме членами следующих групп: администраторы (Administrators), операторы архива (Backup Operators) и операторы сервера (Server Operators)
IPC\$	Сокращение IPC означает «Interprocess Communications» (взаимодействия между процессами). Ресурс предназначен для совместного использования интерфейса именованных каналов, необходимого для работы коммуникационных программ
NETLOGON\$	Общий ресурс используется сервером входа, по умолчанию ему присваивается значение %SystemRoot%\System32\Repl\Import. Используется службой NETLOGON при обработке доменных запросов в Windows Server
Print\$	Используется при управлении общими принтерами
Repl\$	Общий каталог экспортирования, используемый в процессе репликации. По умолчанию присваивается значение %SystemRoot%\System32\Repl\Export

Задание: Выполните ниже предложенные Вам упражнения.

Упражнение 1. Передача каталога в совместное использование

1. В подкаталоге Labs каталога, где установлены материалы курса, дважды щелкните файл Lab2.exe.

2. Правой кнопкой мыши щелкните значок My Computer, во всплывшем меню выберите Explore. Запустится Windows Explorer.

3. На диске C выделите каталог Dos, щелкнув его мышью.

Примечание. Так как это только имитация, каталог dos - единственный, который можно передать в совместное использование.

4. Правой кнопкой мыши щелкните выбранный каталог, во всплывшем меню выберите Sharing. В окне dos Properties щелкните вкладку Share, установите в ней переключатель Shared As.

5. Обратите внимание: раздел Shared As содержит несколько параметров.

Share Name - имя, под которым разделяемый каталог будет виден сетевому пользователю. Если в сети есть компьютеры с операционной системой MS-DOS®, это имя должно отвечать соглашению 8.3 об именах MS-DOS. В сетевой Windows имя не должно превышать 12 символов. По умолчанию именем общего ресурса является имя выбранного каталога.

Примечание. Имейте в виду, что назначаемое Вами имя общего ресурса может отличаться от имени каталога. Но при этом, чтобы получить доступ к сетевому каталогу, необходимо вводить имя общего ресурса, а не имя каталога.

Comment - комментарий (вводить необязательно). Он будет присутствовать рядом с именем ресурса в диалоговом окне Connect Network Drive. User limit — максимальное число пользователей, которые могут одновременно подключиться к сетевому каталогу. По умолчанию ограничений нет.

Permissions (кнопка) — назначение прав доступа к сетевому каталогу.

6. Щелкните кнопку ОК, оставив для общего ресурса имя по умолчанию (Dos). Обратите внимание: появился новый символ - рука, которая держит папку Dos. Это означает, что данный каталог находится в совместном использовании.

Упражнение 2. Отмена совместного использования каталога

1. Щелкните каталог Dos, чтобы выбрать сетевой каталог.

2. Правой кнопкой мыши щелкните выбранный каталог, во всплывшем меню выберите Sharing. Появится окно dos Properties. Щелкните вкладку Share, установите в ней переключатель Not Shared. Обратите внимание: значок (рука, держащая папку) исчез.

3. Щелкните команду Exit Lab 2 в меню File.

2.4. Защита сетевых ресурсов средствами файловой системы

Разделы FAT не обеспечивают локальной безопасности. Именно по этой причине для серверов сетевой Windows по умолчанию запрещается локальный вход для всех учетных записей, не обладающих привилегиями администратора или оператора сервера. Однако для разделов FAT могут устанавливаться общие права, связанные с общим доступом к каталогам в сети. Такая защита не мешает пользователю с локальным входом получить доступ к файлам своего

компьютера, но, по крайней мере, она предотвращает неразрешенный сетевой доступ даже для файлов, находящихся в разделах FAT.

В отношении безопасности NTFS оказывается предпочтительным вариантом. Разделы NTFS могут запрещать или ограничивать доступ как удаленных, так и локальных пользователей. Следовательно, к защищенным файлам смогут обратиться лишь те пользователи, которым были предоставлены соответствующие права.

Общий доступ к каталогам и система безопасности NTFS зависят от атрибутов безопасности, связанных с общим каталогом или любым объектом файловой системы NTFS (который может представлять собой как каталог, так и отдельный файл). Пользователь может выполнить команду File > Properties или щелкнуть на имени файла правой кнопкой мыши и затем выбрать команду Properties из контекстного меню, а затем просмотреть содержимое вкладок Sharing (только для каталогов) и Security (для файлов и каталогов), показанных на рис.2.1 и 2.2.

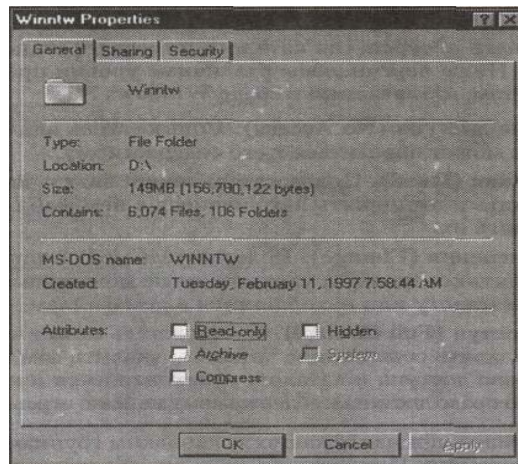


Рис.2.1. Для каталогов отображаются обе вкладки (Sharing и Security)

По умолчанию системной группе Everyone предоставляется полный доступ (Full Control) к общим каталогам и защищенным ресурсам. Только сетевой администратор, владелец или пользователь с правом изменения разрешений (Change Permissions) сможет изменить уровень доступа к общим ресурсам и объектам NTFS.

Права доступа к общим каталогам.

Создание общего ресурса для каталога позволяет подключаться к нему по сети. Ниже перечислены различные уровни прав доступа к общим каталогам, назначаемые в сетевой ОС Windows:

- Отсутствие доступа (No Access). Пользователь видит имя каталога, но не может обратиться к его содержимому.
- Право чтения (Read). Пользователь может видеть имя каталога, может читать и выполнять находящиеся в нем файлы, но не может изменять их.

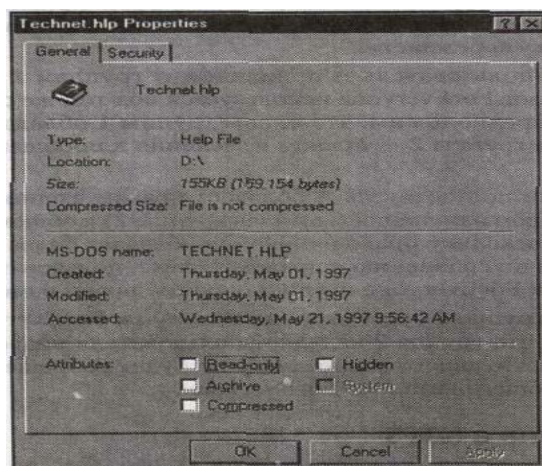


Рис. 2.2. Для файлов отображается одна вкладка (Security)

- Право изменения (Change). Пользователь может читать, записывать и удалять содержимое каталога, но не может изменить права доступа к каталогу или находящимся в нем файлам.
- Полный доступ (Full Control). Пользователь может читать, записывать и удалять содержимое каталога, удалить сам каталог, изменить права доступа к каталогу и находящимся в нем файлам, если только право доступа к содержимому не было ограничено ранее. Для пользователей, принадлежащих нескольким группам, действует принцип поглощения. Исключение составляет отсутствие доступа, отменяющее все остальные права. Иначе говоря, если среди этих прав нет отсутствия доступа, то во всех ситуациях применяется право с наименее жесткими ограничениями; если отсутствие доступа есть, оно всегда «побеждает».

Предположим, пользователь А принадлежит группам 1 и 2. Существующий каталог ForEveryone используется под тем же общим именем. Наконец, предположим, что члены группы 1 обладают правом чтения, а члены группы 2 — правом изменения для общего каталога ForEveryone.

В этой ситуации пользователь А обладает правом чтения (как член группы 1) и правом изменения (как член группы 2) к общему каталогу ForEveryone. Поскольку право изменения обладает более широкими возможностями по сравнению с правом чтения, пользователю А для общего каталога ForEveryone предоставляется право изменения.

Предположим, группе 1 будет запрещен доступ к ForEveryone. Даже несмотря на то, что группа 2 наделяет пользователя правом изменения, из-за существующего запрета ему не будет разрешен доступ к содержимому общего каталога ForEveryone.

Права доступа в NTFS

NTFS рассматривает каталоги (папки) и файлы как разнотипные объекты и ведет отдельные (хотя и перекрывающиеся) списки прав доступа для каждого типа. Ниже перечислены права NTFS, назначаемые папкам (соответствующие права для файлов приведены ниже):

- Нет доступа (No Access) (None) (HeT).
- Полный доступ (Full Control) (A11)(A11) (Все)(Все).
- Право чтения (Read) (RX)(RX) (чтение)(чтение).
- Право добавления (Add) (WX)(Not Specified) (запись/выполнение) (Не указано).
- Право добавления и чтения (Add & Read) (RWX)(RX) (чтение/запись/выполнение) (чтение/выполнение).
- Право просмотра (List) (RX)(Not Specified) (чтение/выполнение)(Не указано).
- Право изменения (Change) (RWXD)(RWXD) (чтение/запись/ выполнение/удаление) (чтение/запись/выполнение/удаление).

Внимание

Обратите внимание на два выражения в скобках, указанные после имени права доступа. Первое выражение относится к самой папке, а второе - ко всем файлам, которые могут быть созданы внутри нее. Например, при полном доступе для папки разрешаются любые действия, однако пользователь с полным доступом к папке также будет обладать полным правом доступа ко всем созданным в ней файлам (если только права доступа к файлу не были изменены его владельцем или администратором). Другими словами, в NTFS файлы и папки по умолчанию наследуют права доступа, установленные для их родительской папки, однако эти права могут быть изменены любым пользователем, которому разрешено изменять права доступа для соответствующих объектов NTFS.

Файлы в NTFS могут обладать следующими правами:

- Полный доступ (Full Control) (All) (Все).
- Нет доступа (No Access) (None) (Нет).
- Право изменения (Change) (RWXD) (чтение/запись/выполнение/удаление).
- Право чтения (Read) (RX) (чтение/выполнение).

Для прав доступа NTFS, как и для прав общих каталогов, действует принцип поглощения. Исключение составляет отсутствие доступа, отменяющее действие всех остальных прав. При

сетевом подключении пользователей права NTFS могут вступить в конфликт с правами общих каталогов. В такой ситуации применяется право доступа с наиболее жесткими ограничениями.

Например, в NTFS на вкладке Security пользователю А был предоставлен полный доступ к папке ForEveryone. Однако на вкладке Sharing пользователю А для той же папки было предоставлено право чтения.

Следовательно, если пользователь А попытается подключиться к папке ForEveryone по сети, он будет обладать лишь правом чтения, потому что из двух прав (NTFS и общего каталога) именно право чтения обладает наиболее жесткими ограничениями. Однако, если пользователь А обратится к папке с того компьютера, на котором находятся файлы, ему будет предоставлено право полного доступа. Это объясняется тем, что права доступа общих каталогов действуют лишь для сетевого доступа.

Для удаленных пользователей применяются как права NTFS, так и права общих каталогов (из которых выбирается право с наиболее жесткими ограничениями). Для локальных пользователей применяются только права NTFS (выбирается право с наименее жесткими ограничениями). Но помните о том, что отсутствие доступа всегда обладает наивысшим приоритетом. Поскольку в Windows NT для NTFS по умолчанию действует право полного доступа, локальный доступ к компьютеру с Windows NT Server обычно разрешается только администраторам и операторам сервера.

Перемещение защищенных файлов в NTFS

Папки более высокого уровня в NTFS обычно обладают теми же правами, что и находящиеся в них файлы и папки. Например, если вы создаете папку внутри другой папки, для которой администраторы обладают правом полного доступа, а операторы архива — правом чтения, то новая папка унаследует эти права. То же относится и к файлам, копируемым из другой папки или перемещаемым из другого раздела NTFS.

Если папка или файл перемещается в другую папку того же раздела NTFS, то атрибуты безопасности не наследуются от нового объекта-контейнера. Например, если из папки с правами чтения для группы Everyone файл перемещается в папку того же раздела с полным доступом для той же группы, то для перемещенного файла будет сохранено исходное право чтения. Дело в том, что при перемещении файлов в границах одного раздела NTFS изменяется только указатель местонахождения объекта, а все остальные атрибуты (включая атрибуты безопасности) остаются без изменений.

Три следующих важных правила помогут определить состояние прав доступа при перемещении или копировании объектов NTFS:

1. При перемещении файлов в границах раздела NTFS сохраняются исходные права доступа.
2. При выполнении других операций (создании или копировании файлов, а также их перемещении между разделами NTFS) наследуются права доступа родительской папки.
3. При перемещении файлов из раздела NTFS в раздел FAT все права NTFS теряются.

Задание: Зарегистрированным пользователям user1, user2, user3 по очереди создать файлы f1, f2, f3 и папку doc.

С помощью команд реализовать следующие правила разграничения доступа к файлам и папке:

	f1	f2	f3	DOC
user1	FC	NA	R	L
user2	R	FC	R	R
user3	C	R	FC	A
Group12	C	FC	R	L
Group23	NA	R	R	A&R

Обозначения в таблице – по первым буквам прав доступа

Проверить бюджеты и их возможности с помощью описанных выше команд

Сделать выводы о корректности реализации правил разграничения доступа.

ЛЗ-03. Контроль за состоянием безопасности информации

Цель: Изучить и научиться практически осуществлять контроль за состоянием безопасности информации.

Учебные вопросы

- 3.1. Средства ведения и анализа системных журналов ОС Windows
- 3.2. Средства контроля за процессами. Свойства процессов и управление ими

Одним из наиболее распространенных способов анализа состояния безопасности вычислительной системы, доступным каждому пользователю, является анализ журналов регистрации событий или журналов аудита /2/.

3.1. Средства ведения и анализа системных журналов ОС Windows

1. Журнал аудита

В операционной системе Windows NT ведется три журнала аудита: журнал безопасности представляет собой файл с именем SecEvent.evt, системный журнал (SysEvent.evt), журнал приложений (AppEvent.evt), расположенные в поддиректории system32/config системной директории. Формат этих файлов недокументирован. Информация хранится в журнале аудита в открытом виде, защита журнала аудита организуется исключительно средствами подсистемы разграничения доступа. Поэтому администраторы Windows NT обязательно должны убедиться, что никто, кроме аудиторов, не имеет доступа к файлу журнала аудита.

Для просмотра журнала аудита используется стандартная утилита Event Viewer, которую можно применять и для просмотра других системных журналов. Эта утилита разрешает читать журнал аудита только членам группы Administrators, а также пользователям, обладающим привилегией аудитора. Эти ограничения доступа действуют и в том случае, когда системный раздел жесткого диска отформатирован под FAT или HPFS. Все пользователи, которые могут читать журнал аудита, могут и очищать его. Факт очистки журнала регистрируется сразу после очистки.

Задание: запустить утилиту Event Viewer (Просмотр событий). Просмотреть формат и содержание отображаемой информации для всех типов журналов. Переключение журналов производится через команду меню Log. Подробности выполнения данной операции и всех перечисленных ниже содержатся в справках соответствующих программ.

Пользователи, не имеющие возможности читать журнал аудита с помощью утилиты Event Viewer, но обладающие правом чтения файла SecEvent.evt, могут читать этот файл с помощью других программных средств. Поэтому права доступа субъектов к этому файлу должны быть ограничены, например, так:

Разрешить	Auditors	все права доступа
Разрешить	SYSTEM	все права доступа

Здесь Auditors - это группа аудиторов, являющаяся подмножеством группы администраторов. Сделать группы аудиторов и администраторов непересекающимися в Windows NT практически невозможно.

Задание: проверить права доступа к указанному файлу стандартными средствами ОС Windows.

Размер журнала аудита по умолчанию ограничен значением 512К, однако администратор операционной системы может установить любое другое значение, кратное 64К. Администратор может также определить поведение операционной системы при переполнении журнала аудита. Возможны три варианта реакции на эту ситуацию:

- 1) старые события стираются по мере необходимости (по умолчанию);

2) если самое старое событие в журнале аудита зафиксировано более N дней назад (число N выбирает администратор), одно или несколько самых старых событий стирается, в противном случае новые события не регистрируются до тех пор, пока не пройдет N дней с момента регистрации самого старого события;

3) новые события не регистрируются до тех пор, пока журнал не будет очищен.

Если значение `CrashOnAuditFail` ключа реестра `\Registry\Machine\SYSTEM\CurrentControlSet\Control\Lsa` равно единице, при переполнении журнала аудита это значение становится равным двум и происходит крах операционной системы ("синий экран"). При следующей загрузке операционной системы в систему может войти только администратор. Он должен очистить журнал аудита, вернуть данное значение реестра в исходное состояние и перезагрузить компьютер. До тех пор пока все эти действия не будут выполнены, подсистема аудита не будет регистрировать события.

Задание: запустить редактор реестра (программа `regedt32.exe` из командной строки), найти указанный ключ, просмотреть значение указанной переменной.

Настройки параметров аудита (указанные выше) просмотреть посредством команды меню `Settings` (Настройки) программы `Event Viewer` (Просмотр событий).

Для добавления записей в журнал аудита используются специальные системные вызовы программного интерфейса `Win32`, пять из которых (`ObjectOpenAuditAlarm`, `ObjectCloseAuditAlarm`, `ObjectPrivilegeAuditAlarm`, `PrivilegedServiceAuditAlarm` и `AccessCheckAndAuditAlarm`) документированы.

Добавлять записи в журнал аудита может лишь субъект доступа, обладающий соответствующей привилегией. По умолчанию эта привилегия предоставляется только псевдопользователю `SYSTEM`, эту установку не следует изменять ни в коем случае. Если эта привилегия предоставляется какому-то физическому пользователю, этот пользователь тем самым получает возможность записывать в журнал аудита произвольную информацию, в том числе и информацию, компрометирующую других пользователей. Обычно новые записи в журнал аудита добавляют ядро, подсистема `Win32` и подсистема аутентификации `Windows`.

2. Политика аудита

Множество событий, информация о которых записывается в журнал аудита, определяется политикой аудита, которую определяют пользователи-аудиторы. `Windows NT` позволяет регистрировать в журнале аудита события следующих категорий:

- вход/выход пользователя из системы;
- доступ субъектов к объектам;
- использование субъектами доступа опасных привилегий;
- изменения в списке пользователей;
- изменения в политике безопасности;
- системные события;
- запуск и завершение процессов.

Для каждого класса событий могут регистрироваться либо только успешные события (соответствующая операция выполнена успешно), либо только неуспешные (при выполнении операции произошла ошибка), либо и те и другие, либо никакие.

В `Windows` считаются опасными следующие привилегии субъектов доступа:

- получать оповещения от файловой системы;
- добавлять записи в журнал аудита;
- создавать маркеры доступа;
- назначать маркеры доступа процессам;
- создавать резервные копии информации, хранящейся на жестких дисках;
- восстанавливать информацию на жестких дисках с резервных копии;
- отлаживать программы.

Далеко не всё объективно опасные привилегии субъектов считаются: опасными с точки зрения подсистемы защиты Windows. Например, не считается опасной привилегия загружать и выгружать драйверы и сервисы.

С другой стороны, в журнале аудита Windows регистрируется использование некоторых других привилегий, которые согласно документации не считаются опасными.

Порядок регистрации событий при доступе субъектов к объектам определяется не только политикой аудита, но и атрибутами защиты объекта. В состав дескриптора защиты может входить системный список контроля доступа (SACL), определяющий порядок регистрации событий аудита при доступе субъектов к данному объекту. Так же как и DACL, SACL представляет собой список переменной длины, элементами которого являются ACE, имеющие следующий формат:

Регистрировать	идентификатор субъекта	права доступа	флаги и атрибуты
----------------	------------------------	---------------	------------------

В отличие от ACE из DACL ACE в SACL всегда имеют тип "регистрирующий ACE" (system audit ACE). Разработчики Windows NT зарезервировали еще один тип ACE - "тревожный" ACE (system alarm ACE), предназначенный для интерактивного оповещения администраторов операционной системы, однако этот механизм до сих пор не реализован.

ACE, входящий в SACL, имеет все флаги, которые имеет ACE, входящий в DACL. Кроме того, ACE из SACL имеют еще два флага:

- **SUCCESSFUL_ACCESS_ACE_FLAG (s)** – если этот флаг установлен, будут регистрироваться в журнале аудита все успешные обращения к объекту субъекта, идентификатор которого записан в ACE, по любому из методов доступа, перечисленных в маске доступа ACE;

- **FAILED_ACCESS_ACE_FLAG (f)** – если этот флаг установлен, будут регистрироваться в журнале аудита все неуспешные обращения к объекту субъекта, идентификатор которого записан в ACE, по любому из методов доступа, перечисленных в маске доступа ACE.

Если в ACE установлены оба флага, регистрируются любые обращения субъекта к объекту по перечисленным методам доступа, как успешные, так и неуспешные. Если в ACE установлен флаг *i*, при доступе субъектов к объекту ACE игнорируется.

Поскольку все ACE в SACL однотипны, порядок их взаимного расположения не имеет значения.

Если в дескрипторе защиты объекта SACL отсутствует, обращения субъектов к этому объекту не регистрируются.

При создании нового объекта SACL назначается объекту по тем же правилам, что и DACL. При наследовании ACE флаги *s* и *f* остаются неизменными.

Для того чтобы событие, связанное с доступом субъекта к объекту, было зафиксировано в журнале аудита, необходимо одновременное выполнение следующих двух условий:

- 1) политика аудита операционной системы допускает регистрацию в журнале аудита событий, связанных с успешным (или неуспешным) доступом субъектов к объектам;

- 2) SACL объекта содержит хотя бы один ACE, в котором:

- идентификатор субъекта относится к субъекту, открывающему объект;
- установлен флаг *s* (или соответственно *f*) и не установлен флаг *i*;
- после отображения отображаемых прав доступа пересечение маски доступа ACE и маски доступа, содержащей права, запрашиваемые субъектом, не пусто.

Таким образом, глобальные настройки политики аудита в отношении доступа субъектов к объектам выполняют роль фильтра, позволяя временно запретить регистрацию успешных/неуспешных попыток доступа всех субъектов ко всем объектам операционной системы.

Задание: создать в своем домашнем каталоге несколько файлов.

Запустить утилиту Диспетчер пользователей (User manager). Посредством команды Политика аудита открыть диалоговое окно, просмотреть возможные параметры настройки политики аудита.

Выполнить команду меню Свойства созданных файлов.

Просмотреть список регистрируемых событий доступа к созданным файлам; назначить аудит дополнительных событий из списка по своему усмотрению.

Открыть файл с помощью соответствующей программы.

Запустить утилиту Просмотр событий (Event Viewer), убедиться в регистрации событий доступа (см. таблицу ниже).

3. Типы регистрируемых событий

Стандартное программное обеспечение Windows позволяет регистрировать в журнале аудита события 52 типов.

Идентификатор	Категория	Описание
512	Системное событие	Перезагрузка операционной системы
513	Системное событие	Завершение работы операционной системы (shutdown)
514	Системное событие	Загрузка пакета аутентификации
515	Системное событие	Запуск процесса аутентификации (в стандартной конфигурации WinLogon.exe)
516	Системное событие	Сбой при регистрации одного или нескольких событий аудита
517	Системное событие	Очистка журнала аудита
518	Системное событие	Загрузка пакета оповещения об изменениях в списке пользователей
528	Вход/выход пользователя из системы	Пользователь успешно вошел в систему
529	Вход/выход пользователя из системы	Вход пользователя в систему запрещен - имя или пароль, введенные при входе в систему, некорректны
530	Вход/выход пользователя из системы	Вход пользователя в домен в данное время запрещен
531	Вход/выход пользователя из системы	Вход пользователя в систему запрещен - учетная запись пользователя заблокирована администратором
532	Вход/выход пользователя из системы	Вход пользователя в домен запрещен - учетная запись пользователя автоматически заблокирована по достижении определенной даты
533	Вход/выход пользователя из системы	Вход пользователя в домен с данной рабочей станции запрещен
534	Вход/выход пользователя из системы	Данный тип (интерактивный, сетевой или сервисный) входа пользователя в систему запрещен
535	Вход/выход пользователя из системы	Вход пользователя в систему запрещен - пароль пользователя устарел
536	Вход/выход пользователя из системы	Пользователь не смог войти в домен из-за сбоев сетевых сервисов
537	Вход/выход пользователя из системы	Пользователь не смог войти в систему по какой-то другой причине
538	Вход/выход пользователя из системы	Пользователь успешно вышел из системы
539	Вход/выход пользователя из системы	Вход пользователя в систему запрещен - учетная запись пользователя автоматически заблокирована из-за превышения максимально допустимого количества попыток входа в систему с неверным паролем
560	Доступ к объекту	Пользователь попытался открыть объект
561	Доступ к объекту	Пользователь закрыл объект
576	Использование опасных привилегий	В маркере доступа пользователя присутствует опасная привилегия
577	Использование опасных привилегий	Предпринята попытка использования опасной привилегии при выполнении операции, не связанной с доступом к объектам
578	Использование опасных привилегий	Предпринята попытка использования опасной привилегии для получения доступа к объекту
592	Запуск/завершение процессов	Запуск нового процесса
593	Запуск/завершение процессов	Завершение процесса

Идентификатор	Категория	Описание
594	Запуск/завершение процессов	Дублирование дескриптора (handle) объекта
595	Запуск/завершение процессов	Непрямой доступ к объекту
608	Изменения в политике безопасности	Субъекту предоставлена новая привилегия
609	Изменения в политике безопасности	У субъекта отнята привилегия
610	Изменения в политике безопасности	Установлены доверительные отношения с другим доменом
611	Изменения в политике безопасности	Доверительные отношения с другим доменом прекращены
612	Изменения в политике безопасности	Изменена политика аудита
624	Изменения в списке пользователей ²	Создана учетная запись нового пользователя
625	Изменения в списке пользователей	Изменен тип учетной записи
626	Изменения в списке пользователей	С учетной записи пользователя снята блокировка
627	Изменения в списке пользователей	Неудачная попытка изменить пароль пользователя
628	Изменения в списке пользователей	Удачная попытка изменить пароль пользователя
629	Изменения в списке пользователей	Учетная запись пользователя заблокирована
630	Изменения в списке пользователей	Учетная запись пользователя удалена
631	Изменения в списке пользователей	Создана новая глобальная группа
632	Изменения в списке пользователей	Пользователь добавлен в глобальную группу
633	Изменения в списке пользователей	Пользователь удален из глобальной группы
634	Изменения в списке пользователей	Глобальная группа удалена
635	Изменения в списке пользователей	Создана новая локальная группа
636	Изменения в списке пользователей	Пользователь добавлен в локальную группу
637	Изменения в списке пользователей	Пользователь удален из локальной группы
638	Изменения в списке пользователей	Локальная группа удалена
639	Изменения в списке пользователей	Произведены изменения в учетной записи локальной группы, не связанные с изменением членства пользователей в этой группе
640	Изменения в списке пользователей	Произведены изменения в списке пользователей, не связанные с редактированием учетных записей
641	Изменения в списке пользователей	Произведены изменения в учетной записи пользователей глобальной группы, не связанные с изменением членства пользователей в этой группе
642	Изменения в списке пользователей	Произведены изменения в учетной записи пользователя, не связанные с изменением типа учетной записи, пароля пользователя и членства пользователя в группах

Процессы, обладающие привилегией добавлять записи в журнал аудита, могут регистрировать события и других (нестандартных) типов. Например, клиент NetWare для Windows регистрирует в журнале аудита системное событие, заключающееся в аутентификации пользователя на сервере NetWare.

4. Администраторы и аудиторы

Архитектура подсистемы аудита Windows неявно предполагает совпадение групп администраторов и аудиторов, что заметно снижает защищенность операционной системы от несанкционированных действий администраторов. Если необходимо сделать группу аудиторов отличной от группы администраторов, следует выполнить следующие действия:

- создать группу по имени, например, Auditors и добавить в нее всех пользователей-аудиторов;

- сделать владельцем файла журнала аудита одного из аудиторов;

- присвоить файлу журнала аудита дескриптор защиты, содержащий DACL вида

разрешить	Auditors	все права доступа
разрешить	SYSTEM	все права доступа

- предоставить группе Auditors привилегию аудитора и отнять эту привилегию у группы Administrators.

После выполнения вышеперечисленных действий просматривать и очищать журнал аудита, а также обращаться к SACL объектов операционной системы могут только пользователи, входящие в группу Auditors.

Поскольку утилита User Manager предоставляет доступ к политике аудита только членам группы Administrators, группа Auditors должна представлять собой подмножество группы Administrators.

Полное разделение группы аудиторов и группы администраторов в Windows с использованием документированных возможностей операционной системы невозможно. Это является существенным недостатком подсистемы аудита ОС Windows.

3.2. Средства контроля за процессами. Свойства процессов и управление ими

Любая современная операционная система в той или иной мере реализует возможности многопрограммного и многопользовательского режимов работы.

Количество процессов, одновременно выполняющихся на одном процессоре, может достигать нескольких десятков. Все ли эти процессы являются надежными с точки зрения безопасности вычислительной системы? Не присутствуют ли в вычислительной системе посторонние процессы, пытающиеся нанести некоторый ущерб вычислительной системе, информационным ресурсам или пользователям?

Это обстоятельство настоятельно требует реализации в составе операционных систем специальных средств управления работой программ и процессов. Как правило, такие средства имеются в составе операционных систем, которые считаются более или менее защищенными.

Рассмотрим реализацию механизмов контроля и управления программами и процессами в операционной системе Windows.

Контроль использования системы с помощью программы Сервер.

Если вы постоянно разрешаете другим пользователям совместное использование файлов и других ресурсов, программа Сервер предоставит интересную и полезную информацию о компьютере. Хотя для того, чтобы предоставить файлы, папки и принтеры в совместное использование, используются их свойства, контроль и управление доступом осуществляются с помощью программы Сервер.

С помощью программы Сервер можно проверить:

- кто подключился к вашему компьютеру;

- какие ресурсы предоставлены в совместное использование;

- кем и какие ресурсы используются;

- репликация каких папок возможна на вашем компьютере;

- кто получает оповещения — уведомления о проблемах, связанных с безопасностью, доступностью ресурсов и доступом к ним.

Программа Сервер является элементом Панели управления. Чтобы запустить ее, щелкните на кнопке Пуск, выберите Настройки (Settings) и щелкните на пункте Панель управления

(Control Panel). После того как появится окно Панели управления, сделайте двойной щелчок на значке Сервер (Server). Появится окно Сервер.

Задание:

Выполнить Контроль за пользователями

Используя Сервер, можно узнать кто и какие ресурсы на вашем компьютере сейчас использует, а также сколько времени прошло с момента подключения пользователя и его последнего обращения к ресурсу.

Чтобы просмотреть эти данные, щелкните в окне Сервер на кнопке Пользователи (Users), и на экране появится окно.

Чтобы просмотреть, какие ресурсы использует пользователь, выберите его имя. Для каждого ресурса показано, сколько раз он открывался и сколько времени он был открыт.

Задание:

Выполнить контроль за ресурсами, предоставленными в совместное использование.

Кнопка Общий доступ (Shares) окна Сервер выводит по сути те же данные, что и кнопка Пользователи, но с другой точки зрения. Щелкнув на кнопке Общий доступ, вы увидите окно диалога.

В первом списке показаны имена ресурсов, число подключенных к ним пользователей и расположение этих ресурсов на вашем компьютере

Во втором списке перечислены все пользователи, подключенные к выбранному ресурсу.

В этом окне, как и в окне Сеансы пользователей (User Sessions), можно отключить от компьютера пользователей по отдельности или группами, воспользовавшись для этого кнопками Отключить (Disconnect) или Отключить все (Disconnect All). Внимательно следите за появляющимися при этом предупреждениями, так как отключение пользователя может привести к потере его данных.

Задание:

Выполнить контроль за использованием ресурсов

Когда вам требуется точно узнать, кто, что и где делает, используйте кнопку Ресурсы (In Use). Щелкнув на ней, вы увидите окно диалога.

В этом окне приводится список всех открытых ресурсов (на уровне файлов, а не предоставленных в совместное использование ресурсов, как в окнах Сеансы Пользователей и Общие ресурсы - Shared Resources) с указанием имени подключившегося пользователя, его режима доступа и пути к ресурсу.

Щелкните на кнопке Обновить, чтобы обновить содержимое окна. Щелкните на этой кнопке Закрывать ресурсы, чтобы отключить выбранного пользователя от выбранного ресурса.

Работая в однопользовательской системе, вы мало задумываетесь о перезагрузке или выключении компьютера. Когда компьютер работает в сети, эти простые действия требуют от вас большего внимания. Если вы предоставляете в совместное использование файлы или другие ресурсы вашего компьютера, вы ответственны не только за предоставление этих ресурсов другим, но и за то, чтобы другие пользователи не теряли свои данные.

Чтобы избежать потери данных и гнева коллег, которых вы оттолкнули от компьютера, возьмите за правило уведомлять всех подключенных к вашему компьютеру пользователей, прежде чем перезагрузить компьютер, закрыть ресурс или отключить пользователей. (Обратите внимание на то, что это не касается разрегистрации. Вы можете разрегистрироваться, и это никак не повлияет на подключенных к вашему компьютеру через сеть пользователей.)

Чтобы предупредить других о том, что вы собираетесь перезагрузить компьютер, сделайте следующее:

1. Щелкните на кнопке Пуск и выберите команду Выполнить (Run).

2. Введите такую команду:

net send /users сообщение.

Эта команда отправит сообщение всем пользователям, подключенным к вашему компьютеру. Вместо слова сообщение введите текст, который вы хотите отправить. Например:

net send /users Закрою систему через 10 минут; будьте готовы

Примечание: чтобы компьютер мог принимать отправляемые по сети сообщения и предупреждения, необходимо, чтобы на нем была запущена Служба сообщений (Windows Messenger). Чтобы выяснить, работает ли она или эту службу нужно запустить, воспользуйтесь значком Службы (Services) окна Панели управления. Если вы администрируете компьютер, которым пользуется несколько человек, убедитесь в том, что они знают об этой службе. Если вы пользуетесь ресурсами, предоставленными в совместное использование на другом компьютере, то проверьте вашу систему и убедитесь в том, что Служба сообщений работает.

Хотя эта возможность системы и не связана напрямую с контролем, программа Сервер обеспечивает также репликацию папок. Папка и содержащиеся в ней файлы могут находиться на сервере (это компьютер с Windows Server), но ее копии могут храниться на рабочих станциях с Windows. Когда выполняется репликация папки, любые изменения в «основной» папке передаются на все рабочие станции, где хранятся ее копии. Таким образом, репликация представляет собой средство централизованного управления файлами и папками, гарантируя при этом наличие точных копий файлов везде, где они требуются. Репликацию папок можно разрешить только на компьютере под управлением Windows Server (компьютер-экспортер). Если вы работаете в Windows Workstation, то можете импортировать папки, но не можете их экспортировать.

Контроль производительности с помощью программы Диспетчер задач.

Диспетчер задач предоставляет простой способ отслеживания основных показателей производительности системы. В частности, в Диспетчере задач сосредоточено внимание на следующих трех показателях:

- использование процессора (CPU);
- использование виртуальной памяти;
- процессы (в грубом приближении они эквиваленты программам).

Диспетчер задач, хотя это весьма полезный инструмент, предоставляет; данные лишь о нескольких показателях. И за исключением графика, на котором представлены результаты деятельности за последние минуты, в нем не отслеживается изменение этих параметров во времени, так что им нельзя воспользоваться для выявления повторяющихся или случайных условий, он лишь показывает, что происходит в данный момент. Когда вам будет недостаточно информации, предоставляемой Диспетчером задач, вы можете обратиться к более мощному средству контроля и отслеживания производительности: Системному монитору.

Как запустить Диспетчер задач.

В отличие от большинства поставляемых с Windows приложений, для Диспетчера задач в Главном меню ярлыка нет. Чтобы запустить Диспетчер задач, выполните одно из следующих действий:

- щелкните правой кнопкой на свободном пространстве Панели задач и выберите в контекстном меню команду Диспетчер задач (Task Manager);
- нажмите Ctrl+Alt+Del, а затем щелкните на кнопке Диспетчер задач (Task Manager). (При нажатии клавиш Ctrl+Alt+Del все окна с экрана исчезнут и появится окно Безопасность Windows NT — Windows NT Security. Не волнуйтесь. Как только вы щелкнете на кнопке Диспетчер задач, все старые окна появятся снова и откроется окно Диспетчера задач).

Когда вы запускаете Диспетчер задач в первый раз, в его окне выбрана вкладка Приложения (Applications).

В основной части окна приведен список всех запущенных приложений, а также их состояние. В строке состояния выводятся сведения о числе выполняемых процессов, использовании процессора и виртуальной памяти.

Можно выбрать приложение и переключиться на него или завершить его, щелкнув на соответствующей кнопке.

Вкладка Процессы (Processes), содержит список выполняющихся процессов. Чтобы увидеть эту вкладку, щелкните на ее корешке.

Процессом (process) называется выполняемая программа (например, Проводник Windows или Microsoft Word), служба (работа с которой осуществляется при помощи значка Службы ок-

на Панели управления, например Служба сообщений) или подсистема (например, подсистема для выполнения приложений Windows 3.x).

Эту вкладку можно использовать для просмотра выполняемых процессов и выявления процессов, доминирующих в использовании процессора и виртуальной памяти.

По умолчанию на вкладке Процессы для каждого процесса выводятся следующие сведения:

- Имя образа (Image Name): имя процесса;
- PID: идентификатор процесса (его ID), уникальное число, идентифицирующее процесс во время его выполнения;
- CPU: время использования процессом процессора (в процентах);
- CPU-время (CPU Time): время (в секундах), в течение которого выполняется процесс;
- Память (Mem Usage): объем памяти (в килобайтах), используемой процессом;

Можно просмотреть и другие столбцы. Для этого, находясь на вкладке Процессы, выберите в меню Вид команду Выбор столбцов (Select Columns).

3.3. Анализ настройки системы разграничения доступа в среде ОС Windows

В качестве средства автоматизации процесса моделирования системы разграничения доступа (СРД) в АРМ пользователей к объектам доступа (ресурсам файловой системы АРМ и периферийным устройствам, а также к ресурсам локальной вычислительной сети) применяется программное средство «Анализатор уязвимостей «НКВД 2.3» /4/.

Задание:

1. Изучить теоретический материал из описания применения «Анализатора уязвимостей «НКВД 2.3».
2. Войти в систему под именем, выданным администратором.
3. Зарегистрировать три пользователя с учетными записями user1, user2, user3.
4. Создать локальные группы Group12, содержащую первого и второго пользователя, и Group23, куда будут входить пользователи user2 и user3 соответственно.
5. Зарегистрированным пользователям user1, user2, user3 поочередно создать папки f1, f2, f3, f4 и в них файлы 1.doc – 4.doc.
6. С помощью команд реализовать следующие правила разграничения доступа к файлам и папке:

	f1	f2	f3	f4
user1	FC	NA	R	L
user2	R	FC	R	R
user3	C	R	FC	A
Group12	C	FC	R	L
Group23	NA	R	R	A&R

Обозначения в таблице – по первым буквам прав доступа.

7. Проверить бюджеты и их возможности с помощью команд, рассмотренных на занятии 2/7.
8. Выполнить с помощью анализатора уязвимостей «НКВД 2.3» следующие функции:
 - сканирование ресурсов файловой системы АРМ (введенных каталогов, файлов), доступных пользователю АРМ;
 - автоматическое построение по результатам сканирования структуры объектов доступа, для каждого зарегистрированного пользователя;
 - вывод на экран структуры объектов доступа и таблицы полномочий доступа к объектам доступа.
9. Сделать выводы о корректности реализации правил разграничения доступа.

Для автоматизации проверки соответствия полномочий, предоставляемых пользователям системой защиты информации аттестуемой АС по доступу к объектам доступа (ресурсам файловой системы ОС и периферийным устройствам, а также к ресурсам АС), полномочиям поль-

зователей, указанным в модели системы разграничения доступа (СРД), разработанной средством моделирования «Анализатор уязвимостей «НКВД 2.3». применяется программное средство «Анализатор уязвимостей «НКВД 2.2» /3/.

Задание:

1. Ознакомиться с порядком работы с программой «Анализатор уязвимостей «НКВД 2.2».

2. С помощью «Анализатора уязвимостей «НКВД 2.2» выполнить следующие функции:

- сравнение данных, полученных сканированием структуры объектов доступа с данными, указанными в описании модели СРД пользователей к объектам доступа;

- проверку установленных в модели СРД АРМ полномочий пользователей по доступу к объектам доступа на соответствие установленным ПРД.

- проверку реального предоставления пользователям АРМ системой защиты информации полномочий по доступу к объектам доступа в соответствии с установленными моделью СРД полномочиями.

- планирование проверки реальных полномочий пользователей по отношению к объектам доступа осуществлять только для созданных каталогов. Для этого из плана исключаются все объекты, кроме f1, f2, f3, f4, по отношению к которым будут выполнены попытки доступа пользователей.

3. По результатам проверок сформировать соответствующие протоколы аттестационных испытаний в виде текстовых файлов.

ЛЗ-04. Исследование проблем очистки магнитных носителей

Цель: Изучить и освоить технологию уничтожения и восстановления файлов на магнитных носителях. Выполнить задания ЛЗ и представить результаты их выполнения преподавателю.

Учебные вопросы:

- 4.1. Восстановление удаленных файлов
- 4.2. Восстановление отформатированных дискет
- 4.3. Средства освобождения областей оперативной памяти и внешних накопителей

4.1. Восстановление удаленных файлов

При выполнении команды уничтожение файла DELETE операционная система MS DOS - осуществляет всего две операции:

- уничтожает соответствующее уничтожаемому(ым) файлу(ам) пространство таблицы его (их, т.е. файлов) размещения;
- заменяет первый символ имени файла в каталоге на символ?.

Следовательно, на диске по-прежнему сохраняется содержимое удаленных файлов, однако просмотреть его обычными средствами не возможно.

Просмотреть содержание удаленных файлов или просто просмотреть содержание пространства на магнитном диске, считающегося свободным, можно с помощью специальных программ, например, "Крот-М" или "Terrier" /5, 6/.

Задание 1:

1. Ознакомиться с порядком работы с программами "Крот-М" (в каталоге ...\\Крот-1М\\ файл "Крот-мис.txt") и "Terrier" (в каталоге ...\\Terrier\\ файл "Описание применения Terrier.doc").
2. Подготовить отформатированную дискету. Скопировать на нее несколько текстовых файлов.
3. Выполнить операцию удаления файлов.
4. Открыть программу "Крот-1М" и просмотреть с ее помощью содержимое свободного пространства диска A:, двумя способами:
 - выполнив поиск по ключевым словам на свободном пространстве;
 - просмотрев содержание соответствующих удаленному файлу физических секторов.
5. Просмотреть содержимое диска A: при помощи программы "Terrier".
6. Запустить программу UnErase Wizard командой:
 Пуск->Программы->Norton Utilities->UnErase Wizard.
7. Последовательно выполняя шаги при помощи кнопки [Далее>], восстановить удаленные файлы. Завершить выполнение программы нажатием клавиши [Готово].
8. Просмотреть содержание восстановленных файлов и убедиться в правильности восстановления.
9. Снова удалить несколько файлов и скопировать на их место один или два файла меньшего размера.
10. Запустить программу UnErase Wizard как указано выше. Просмотреть информацию об удаленных файлах и попытаться их восстановить.
11. Проанализировать результаты выполнения обеих операций.

4.2. Восстановление отформатированных дискет

Для исследования возможности восстановления информации на ошибочно отформатированных дискетах воспользуемся программой UnFormat, входящей в состав Norton Utilities и являющейся DOS – приложением.

Задание 2:

1. Подготовить отформатированную дискету и скопируйте на нее несколько текстовых файлов.

2. Выполнить быстрое форматирование дискеты средствами ОС WINDOWS.
3. Просмотреть содержимое диска A: при помощи программ "Terrier" и "Крот-М".
4. Перезагрузить компьютер в режиме MS-DOS и запустите программу UnFormat командой: ... \NU\unformat a:
Подтвердите свое желание восстановить дискету в ответ на запросы программы, на вопрос программы: использовали ли вы ранее программы типа IMAGE.EXE?, ответьте: НЕТ.
Зафиксируйте все сообщения программы.
Если программа UnFormat рекомендует выполнить программу UnErase, сделайте это.
5. Просмотреть восстановленные файлы на дискете и убедиться в правильности восстановления информации в них.
6. Повторить пункты 1-5, выполнив в пункте 2 полное форматирование.
7. Проанализировать результаты работы программы UnFormat в обоих случаях и сделать выводы.

4.3. Средства освобождения областей оперативной памяти и внешних накопителей

Наличие информации на якобы свободном пространстве магнитного диска способно привести к утечке информации. Поэтому, для гарантированного стирания информации необходимо применять специальные программные средства. Например, такими возможностями обладают программа "Крот-М" и программа Wipe Info из пакета Norton Utilities.

ВНИМАНИЕ! СТЕРТЫЕ ФАЙЛЫ ВОССТАНОВЛЕНЫ БЫТЬ НЕ МОГУТ! ВЫПОЛНЕНИЕ ЗАДАНИЙ – ТОЛЬКО НА ГИБКОМ МАГНИТНОМ ДИСКЕ!

Задание 3:

1. Запустить программу Wipe Info командой:
Пуск->Программы->Norton Utilities->Wipe Info.
2. На вопрос с экрана "Что вы хотите стереть?" ответить [Свободное пространство] и нажать затем кнопку [Далее].
3. Внизу в опции "Выберите диск:" выбрать в списке диск A: и нажать кнопку [Далее].
4. На следующем экране в качестве метода стирания выбрать [Быстрое очищение] и нажать кнопку [Далее].
5. Просмотреть содержимое диска A: при помощи программы "Terrier". Элементы каталога, соответствующие удаленным файлам, остались, а местонахождение их – не определено. Просмотрите неиспользуемое пространство диска и убедитесь, что информации на диске не осталось.

Задание 4: Выполнить задание 3, поэкспериментировав с возможными вариантами опций во 2 и 4 пунктах. После каждого этапа не забудьте просматривать содержимое диска A: при помощи программы "Terrier".

Замечание: Wipe Info поддерживает два режима стирания:

- "Быстрое" очищение с возможностью выбора значения величины, которая записывается вместо стертых данных;
- "Правительственное очищение", соответствующее процедуре Очищения, определенной в документе 5220-22-М (Руководство к Программе Национальной Промышленной Безопасности) МО США (DoD) с возможностью выбора числа повторений записи и значения величины (0-255), которая используется в качестве образца в двоичном формате для данных, записываемых вместо стертых.

Аналогичные операции по чистке неиспользуемого пространства магнитных дисков может выполнять и программа «Крот-1М».

Задание 5:

1. Запустите программу «Крот-1М» и выполните операцию очистки свободного пространства диска самостоятельно.
2. Просмотрите состояние диска с помощью программы «Крот-1М».
3. Закройте все программы.

Подготовить отчет по результатам выполнения ЛЗ-02.

Отчет по лабораторной работе должен содержать:

- содержание работы и перечень использованных технических и программных средств;
- протоколы работы программ и результаты их работы с подробным анализом результатов;
- выводы по проделанной работе с точки зрения обеспечения безопасности информации от ее несанкционированного получения.
- отчет за 10 минут до конца занятия представить преподавателю.

Быть готовым к ответу на вопросы по результатам исследований.

ЛЗ-05. Средства ЗИ от разрушающих программных воздействий (РПВ)

Цель: Изучить и опробовать средства ЗИ от разрушающих программных воздействий. Студенты уясняют и выполняют задания ЛЗ и выполняют все работы по ним

Учебные вопросы:

- 5.1. Средства анализа программ
- 5.2. Дизассемблирование программ и исследование кода

Литература:

5.1. Средства анализа программ

Одним из средств анализа программ является комплекс программ дизассемблирования “SOURCER”, который позволяет из исходных исполняемых модулей (.COM или .EXE файлы), а также драйверов устройств получить их исходный текст в виде

- листинга или
- .ASM - файла.

Исходный ассемблерный текст программы может быть построен в удобном для обработки виде в зависимости от используемого транслятора: MASM, TASM различных версий.

Полученный файл может быть подвергнут анализу, изменен и повторно ассемблирован.

Для изучения возможностей по дизассемблированию программ разработан тестовый пример на языке ассемблера (см. рис.5.1):

```
.MODEL SMALL
.STACK 100h
;-----
.DATA
TP      DB      'Is it after 12 noon (Y/N)? $'
GMM     DB      13,10, 'Good morning, world!' , 13 , 10 , '$'
GAM     DB      13,10, 'Good afternoon, world!' , 13 , 10 , '$'
;-----
.CODE
mov ax,@data
mov ds,ax                ;установка DS на начало сегмента данных
mov dx,OFFSET TP         ;в DX - смещение TP
mov ah,9                 ;функция печати строки
int 21h                  ;вывод строки на стандартный выход
mov ah,1                 ;функция чтения символа
int 21h                  ;чтение символа
cmp al,'y'               ;сравнение в нижнем регистре?
jz IsAfternoon           ;yes, it's after noon
cmp al,'Y'               ; сравнение в верхнем регистре
jnz IsMorning            ;no, it's before noon
IsAfternoon:
mov dx,OFFSET GAM        ;загрузка смещения GAM
jmp Displ
IsMorning:
mov dx,OFFSET GMM        ; загрузка смещения GMM
Displ:
mov ah,9                 ; функция печати строки
int 21h                  ; вывод строки на стандартный выход
mov ah,4ch               ; функция завершения программы
int 21h                  ; завершить программу
END
```

Рис.5.1 Исходный текст программы

Для практической отработки вопросов дизассемблирования и анализа программ предлагается:

- ассемблировать предложенный исходный текст;
- собрать его в исполняемый модуль;
- исходный текст переименовать для последующего исследования;
- запустить полученную программу на выполнение для анализа производимых действий;
- дизассемблировать полученный модуль;
- сравнить его исходный текст, полученный дизассемблером с сохраненным исходным текстом;
- сделать соответствующие выводы.

5.2. Дизассемблирование программ и исследование кода

Для выполнения работы выполните следующие действия:

- загрузите компьютер;
- перейдите в каталог SOURCER;

Дальнейшие действия должны выполняться в четкой последовательности:

1. Внимательно изучите исходный текст программы PZ43.ASM и обратите внимание на основные блоки программы и секции, а так же на приводимые комментарии. Уточните, какие прерывания используются в программе и их назначение.

2. Используя ассемблер TASM.EXE получите из исходного текста PZ43.ASM объектный модуль PZ43.OBJ:

```
c:\source\tasm.exe pz43      <Enter>
```

в результате трансляции будет получен файл PZ43.OBJ.

3. Используя редактор связей TLINK.EXE получите из объектного модуля PZ43.OBJ исполняемый модуль PZ43.EXE:

```
c:\source\tlink.exe pz43      <Enter>
```

В результате редактирования межпрограммных связей будет получен файл PZ43.EXE.

4. Для дальнейшего анализа сохраните исходный текст PZ43.ASM под другим именем, например:

```
c:\source\ren pz43.asm pz43.old      <Enter>
```

5. Запустите полученный исполняемый модуль на выполнение:

```
c:\source\pz43.exe <Enter>
```

Проследите все этапы выполнения программы.

6. Запустите дизассемблер на полученный модуль PZ43.EXE с целью получения исходного текста программы на языке ассемблера:

```
c:\source\sr.exe pz43.exe      <Enter>
```

После запуска дизассемблера раскроется главное окно дизассемблера, в котором можно задать режимы работы. Подсвеченные буквы являются ключевыми для соответствующих режимов работы программы и нажатие на них позволяет изменить работу дизассемблера:

O	-	изменение имени выходного файла
H	-	включение пользовательского заголовка в выходной файл
S	-	форма представления адресов в листинге
N	-	включение / выключение кодов команд в 16 с.с.
W	-	стиль букв (верхний/нижний регистр)
L	-	изменение форматов меток
R	-	комментарии
T	-	выбор версии транслятора (многократным нажатием клавиши T добейтесь TASM 2.X)
U	-	выбор процессора (многократным нажатием клавиши U добейтесь 486 REAL)
D	-	диск для записи выходного файла
C	-	тип исполняемого модуля .COM или .EXE

F - формат выходного файла .ASM или .LST (выберите .ASM)
 G - запуск на дизассемблирование

7. Запустите дизассемблер на создание исходного текста программы на языке ассемблера, нажав клавишу G.

Если запуск дизассемблера производится не первый раз для одной и той же программы, будет выдано предупреждение о существовании выходного файла. Ответьте Y для перезаписи.

В результате получите исходный текст дизассемблированной программы (рис.5.2):

8. Внимательно просмотрите оба исходных текста PZ43.OLD и PZ43.ASM. Какие в них отличия?

9. Переименуйте старый PZ43.EXE в PZ43_L.EXE для последующего анализа.

10. Оттранслируйте и соберите новый исполняемый модуль из полученного дизассемблерного текста:

c:\source\tasm.exe pz43 <Enter>

c:\source\tlink.exe pz43 <Enter>

Получится новый PZ43.EXE .

PAGE 59,132

```
#####
;##                                     ##
;##                                PZ43    ##
;##                                     ##
;## Created: 7-Jan-97                    ##
;## Passes: 5 Analysis  Options on: none    ##
;##                                     ##
#####
target      EQU 'T2' ; Target assembler: TASM-2.X
include srmacros.inc
.486c
.387
;----- seg_a -----
seg_a      segment      byte public use16
            assume cs:seg_a , ds:seg_a , ss:stack_seg_c
;#####
;
; Program      Entry Point
;
;#####
pz43      proc    far
start:
            mov     ax,seg_b
            mov     ds,ax
            mov     dx,offset data_2      ; ('Is it after 12 noon (Y/N)')
            mov     ah,9
            int     21h                    ; DOS Services ah=function 09h
                                           ; display char string at ds:dx

            mov     ah,1
            int     21h                    ; DOS Services ah=function 01h
                                           ; get keybd char al, with echo

            cmp     al,79h                  ; 'y'
            je      short loc_1            ; Jump if equal
            cmp     al,59h                  ; 'Y'
```

```

    jne     short loc_2          ; Jump if not equal
loc_1:
    mov     dx,34h
    jmp     short loc_3
                                ;* No entry point to code
    nop
loc_2:
    mov     dx,offset data_3     ; (")
loc_3:
    mov     ah,9
    int     21h                  ; DOS Services ah=function 09h
                                ; display char string at ds:dx
    mov     ah,4Ch
    int     21h                  ; DOS Services ah=function 4Ch
                                ; terminate with al=return code
    db      7 dup (0)
pz43
seg_a      ends
;----- seg_b ----

seg_b      segment             byte public use16
            assume cs:seg_b , ds:seg_b , ss:stack_seg_c

data_2     db      'Is it after 12 noon (Y/N)?$'
data_3     db      0Dh, 0Ah, 'Good morning, world!', 0Dh
            db      0Ah, '$'
            db      0Dh, 0Ah, 'Good afternoon, world!'
            db      0Dh, 0Ah, '$'
            db      0
seg_b      ends
;----- stack_seg_c ----

stack_seg_c segment            word stack 'STACK' use16
            db      256 dup (0)
stack_seg_c ends
            end      start

```

Рис.5.2. Дизассемблированный текст программы.

11. Запустите полученный исполняемый модуль на выполнение:

c:\source\pz43.exe <Enter>

а затем старый:

c:\source\pz43_1.exe <Enter>

Сравните работу двух моделей.

Сравните размеры нового и старого модуля.

Почему размеры отличаются? Сделайте выводы.

ЛЗ-06. Применение программных антивирусных комплексов

Цель: Изучить и практически опробовать наиболее известные антивирусные программы. Студенты уясняют и выполняют задания ЛЗ и выполняют все работы по ним

Учебные вопросы:

- 6.1. Настройка антивирусных программных комплексов
- 6.2. Применение антивирусных программных комплексов

Литература:

6.1. Настройка антивирусных программных комплексов

1.1. Семейство антивирусных программ Dr.WEB

Программы семейства Dr.WEB выполняют поиск и удаление известных им вирусов из памяти и с дисков компьютера, а также осуществляют эвристический анализ файлов и системных областей дисков компьютера /7/. Эвристический анализ позволяет с высокой степенью вероятности обнаруживать новые, ранее неизвестные, компьютерные вирусы.

В комплект программ для Windows 95-XP входит:

- полифаг Dr.WEB;
- резидентный сторож SpIDer Guard и начиная с версии 4.20
- планировщик Dr.WEB.

Dr.WEB представляет собой классический полифаг и предназначена для использования в 32-битных операционных системах семейства Windows (т.е. Windows 95/98/2000/ME/XP, а также Windows NT 4.0 и выше). Программа производит сканирование файлов и системных областей дисков компьютера на наличие в них компьютерных вирусов и, при нахождении последних, производит их лечение. Кроме того, в составе программы имеется эвристический анализатор, позволяющий находить новые, неизвестные вирусы.

SpIDer Guard является резидентной антивирусной программой (сторож), работающей под операционными системами Windows 9x/2000/ME/XP, а также Windows NT 4.0 и выше. SpIDer Guard перехватывает обращения к файлам и системным областям дисков, осуществляя проверку на наличие в них компьютерных вирусов "на лету". При обнаружении вируса SpIDer Guard предпринимает действия по обезвреживанию (лечению, удалению, перемещению в заранее заданную область) или блокированию инфицированного файла (запрещение доступа к инфицированному файлу). Действия могут предприниматься в автоматическом (без вмешательства пользователя) или полуавтоматическом режимах. В полуавтоматическом режиме пользователь самостоятельно определяет тип конкретного действия с инфицированным файлом. Таким образом, при активизированном стороже, доступ к файлам и/или системным областям разрешается только в случае, если вирусы не обнаружены, либо их удалось обезвредить. Кроме того, в SpIDer Guard предусмотрен специальный режим работы - обнаружение и блокирование вирусной активности. При активизации этого режима SpIDer Guard способен обнаружить и заблокировать попытки неизвестных и неопределяемых эвристическим анализатором компьютерных вирусов производить повторное инфицирование объектов на дисках компьютера.

Планировщик Dr.WEB, позволяет производить запуск антивирусных программ и проверку устройств хранения информации, а также осуществлять обновление вирусных баз и компонентов программы по графику, задаваемому пользователем.

Настройка программы DrWeb. Для вызова окна настроек программы можно воспользоваться кнопкой [Настройки] в главном окне, пунктом меню *Настройки -> Изменить установки*, или горячей клавишей F9. Окно настроек включает следующие закладки:

- проверка;
- типы;
- действия;

- архивы;
- отчет;
- пути;
- события;
- обновления;
- общие.

Закладка «Проверка». На этой закладке определяются настройки антивирусного сканирования.

Переключатель [Эвристический анализ] включает или выключает эвристический анализ, позволяющий производить поиск и обнаружение новых, неизвестных Dr.WEB вирусов. Уникальный эвристический анализатор производит запуск проверяемых программ в модели операционной системы, контролируя и анализируя все действия тестируемого объекта. При обнаружении подозрительного действия, пользователю выводится предупреждение о возможном заражении объекта определенным типом вируса. Выключение этой опции увеличивает скорость работы программы, однако поиск вирусов в этом случае производится лишь на основе записей, имеющихся в основной и дополнительных вирусных базах.

Переключатель [Проверять память] позволяет в режиме по умолчанию включать или отключать проверку оперативной памяти компьютера на наличие активного резидентного вируса при запуске программы. Для проверки памяти при уже запущенной программе можно воспользоваться меню *Файл -> Проверить память* или горячей клавишей *F6*.

Переключатель [Проверять загрузочные сектора] позволяет в режиме по умолчанию включать или отключать проверку загрузочных секторов дисков на наличие в них вирусов.

Переключатель [Проверять подкаталоги] позволяет в режиме по умолчанию включать или выключать проверку файлов во вложенных подкаталогах.

Переключатель [Проверка нескольких дискет] инициирует выдачу предложения проверки следующей дискеты после завершения анализа текущей.

Переключатель [Запрос подтверждения всегда] инициирует выдачу запроса на подтверждение любого действия, которое собирается предпринять Dr.WEB.

Закладка «Типы». На этой закладке определяются типы файлов, подлежащих тестированию.

С помощью переключателей, объединенных в группу под названием *Режим проверки*, задаются типы проверяемых файлов.

При включении опции *Все файлы* будет производиться проверка всех файлов без исключения, в том числе текстовых, графических, баз данных и т.д. Эта работа может занять слишком много времени. Рационально производить такую проверку лишь при первичной установке программы.

Опция *По формату* позволяет производить отбор файлов на тестирование в соответствии с их внутренним форматом, без учета расширения. Исполняемый инфицированный файл может быть переименован, например в текстовый, для уклонения от тестирования антивирусными программами, работающими только по расширению файлов.

При включении опции *Выбранные типы* отбор файлов на тестирование производится в соответствии со списком расширений, приведенном в правой панели. С помощью кнопок *Добавить* и *Удалить* данный список можно редактировать, а кнопкой *Базовый* можно вернуться к списку, заданному по умолчанию.

Опция *Заданные маски* позволяет производить отбор файлов для тестирования, имена которых подходят под определенные маски, заданные в дополнительном, редактируемом списке, приведенном в правой панели. С помощью кнопок *Добавить* и *Удалить* можно редактировать этот список, а кнопкой *Базовый* можно вернуться к списку, заданному по умолчанию.

Три переключателя, находящиеся на этой закладке - [Файлы в архивах], [Упакованные файлы] и [Почтовые файлы], включают проверку файлов в архивах (ZIP, ARJ, RAR, TAR, GZIP и CAB), упакованных файлов (DIET, LZEXE, PKLITE, EXEPACK, COMPACK, OPTLINK,

WWPACK, WWPACK32, PMGPAK, UCEXE) и почтовых вложений в формате UUE и MIME соответственно.

ВНИМАНИЕ: лечение инфицированных файлов в архивах и почтовых вложениях не производится.

Закладка «Действия». На этой закладке определяются действия, которые Dr.WEB будет производить с инфицированными, неизлечимыми и подозрительными файлами.

В верхней части закладки размещены три кнопки выбора категории файлов, для которых ниже можно определить действия Dr.WEB:

[Для инфицированных] [Для неизлечимых] [Для подозрительных]

Справка:

- под инфицированным понимается файл, содержащий в себе тело вируса, известного программе Dr.WEB. Излечение такого файла возможно.
- под неизлечимым понимается файл, содержащий в себе тело вируса, известного программе Dr.WEB. Причем излечение такого файла невозможно по причине необратимого инфицирования.
- под подозрительным понимается файл, проверка которого вызвала срабатывание эвристического анализатора Dr.WEB. Такой файл может содержать вирус, неизвестный Dr.WEB.

Для любой категории файлов действия, предпринимаемые программой определяются с помощью набора переключателей.

Выбор опции [Информировать] приведет к тому, что программа при обнаружении файлов соответствующей категории будет лишь информировать пользователя об обнаружении вируса или подозрении о его наличии.

При выборе опции [Вылечить] Dr.WEB, обнаружив инфицированный файл, будет пытаться его вылечить. Данная опция недоступна для неизлечимых и подозрительных файлов.

При выборе опции [Удалить], [Переименовать] или [Переместить в], файл, в котором Dr.WEB определил наличие вируса, будет удален, переименован или перемещен соответственно. Переименование будет осуществлено путем замены расширения файла на другое, заданное в поле справа от опции [Переименовать]. Перемещение будет произведено в каталог, путь к которому указан в поле справа от опции [Переместить в]. С помощью [...] кнопки можно задать путь, не вводя его вручную.

Флажок [Запрос подтверждения] отвечает за выдачу пользователю запроса для подтверждения выполнения заданного действия после обнаружения инфицированного, неизлечимого или подозрительного файла.

Закладка «Архивы»

На этой закладке определяются действия, которые Dr.WEB будет производить с инфицированными, неизлечимыми и подозрительными файлами, обнаруженными в архивах, почтовых файлах и контейнерах.

В верхней части закладки размещены три кнопки выбора категории файлов, для которых ниже можно определить действия Dr.WEB:

[Для архивов] [Для почтовых файлов] [Для контейнеров]

Для любой категории действия, предпринимаемые программой при обнаружении инфицированного, неизлечимого и подозрительного файла, определяются с помощью набора переключателей.

Выбор опции [Информировать] приведет к тому, что программа при обнаружении инфицированного, неизлечимого и подозрительного файла будет лишь информировать пользователя об обнаружении вируса или подозрении о его наличии.

При выборе опции [Переименовать] или [Переместить в], архив, почтовый файл или контейнер, в котором Dr.WEB определил наличие вируса, будет переименован или перемещен соответственно. Переименование архива, почтового файла или контейнера будет осуществлено путем замены расширения файла на другое, заданное в поле справа от опции [Переименовать]. Перемещение будет произведено в каталог, путь к которому указан в поле справа от опции [Переместить в]. С помощью кнопки [...] можно задать путь, не вводя его вручную.

Флажок [Запрос подтверждения] отвечает за выдачу пользователю запроса для подтверждения выполнения заданного действия после обнаружения инфицированного, неизлечимого или подозрительного файла.

Закладка «Отчет». На этой закладке определяется файл отчета, формируемый при работе программы DrWeb и производится настройка его параметров.

С помощью переключателя [Вести файл отчета] можно запретить или разрешить формирование программой Dr.WEB файла отчета. Имя формируемого файла задается в поле редактирования, приведенном ниже переключателя.

С помощью группы переключателей [Режим открытия отчета] определяется режим ведения файла отчета:

- добавлять новые записи к уже существующим записям;
- перезаписывать файл заново, в этом случае записи, внесенные в отчет при предыдущих сеансах работы, теряются.

С помощью группы переключателей [Кодировка] задается вариант используемой кодировки русских символов при записи в файл отчета:

- ANSI соответствует кодировке, используемой в Windows. Использование данной кодировки позволяет открывать созданные Dr.WEB файлы отчета с помощью программ просмотра или редактирования для Windows (например, программой NotePad).

- OEM соответствует кодировке, применяемой в DOS. Использование данной кодировки удобно при открытии файла отчета, например, программой просмотра DOS-Navigator'a.

В группе [Детали] можно определить степень детальности информации, записываемой в файл отчета. Включение опции *Проверяемые объекты* приводит к включению в отчет имени каждого проверяемого объекта. Это значительно увеличивает размер создаваемого файла.

Установка [Предельного размера файла отчета] позволяет ограничить размер файла до объема, заданного пользователем. При превышении предельного размера, файл будет начат сначала.

Закладка «Пути». На этой закладке определяются каталоги (папки), внутри которых антивирусная проверка файлов производится не будет, а также задаются пути к вирусным базам программы Dr.WEB.

Практически у каждого пользователя на жестком диске присутствует каталог, а то и несколько, в которых хранятся файлы архивного назначения. Проверка этих каталогов на наличие вирусов при каждом запуске Dr.WEB'a будет занимать дополнительное время. На данной закладке можно определить список каталогов, в которых файлы проверяться не будут.

Для внесения каталога в список исключенных из анализа необходимо ввести полный путь к данному каталогу в поле ввода *Список исключаемых путей* (или нажав кнопку [...], отметить нужный каталог и нажать Ok), а затем подтвердить выбор кнопкой *Добавить*. Для удаления каталога из списка достаточно нажать ▼ и в появившемся списке выбрать исключаемый каталог, подтвердив действие кнопкой *Удалить*.

Вирусные базы Вы можете хранить в каталоге, отличном от местонахождения программы Dr.WEB. В этом случае имеется возможность определения дополнительных путей поиска вирусных баз.

Для внесения каталога в список путей поиска вирусных баз, необходимо ввести полный путь к данному каталогу в поле ввода *Список путей к вирусным базам* (или нажав кнопку [...]) отметить нужный каталог и нажать Ok), а затем подтвердить выбор кнопкой *Добавить*. Для удаления каталога из списка достаточно нажать ▼ и в появившемся списке выбрать исключаемый каталог, подтвердив действие кнопкой *Удалить*.

Закладка «События». На этой закладке можно определить звуковые эффекты, которые могут сопровождать события, происходящие в процессе работы программы, на компьютере, оборудованном звуковой картой.

Для каждого события, выпадающий список которых появляется при нажатии на кнопку ▼, может быть сопоставлен звуковой файл в формате WAV. Выбрав в списке событие, доста-

точно ввести имя звукового файла в поле ввода справа. Для быстрого поиска и ввода имени звукового файла можно воспользоваться кнопкой [...].

Закладка «Обновление». На этой закладке устанавливаются параметры, необходимые для автоматического обновления Dr.WEB через Internet или локальную сеть.

Для работы подсистемы автоматического обновления в поле ввода *Адрес сервера обновления* должен быть введен адрес расположения удаленной системы обновления. В качестве такого адреса может быть задано:

- HTTP URL. Обновление через Internet поддерживается только по протоколу HTTP. По умолчанию подсистема обновления настроена на обращение к коммерческому разделу www-сервера ООО "СалД" "http://www.drweb.ru/ftp/update". С таким URL обновление доступно только для зарегистрированных пользователей программы Dr.WEB, имеющих персональные атрибуты для доступа к данному ресурсу сети - имя пользователя и пароль. В этом случае персональные атрибуты должны быть определены в полях *Имя пользователя* и *Пароль*. Для пользователей, имеющих демонстрационные и ознакомительные версии программы, адрес сервера обновления необходимо изменить на обращение к некоммерческому разделу www-сервера ООО "СалД" - "http://www.drweb.ru/ftp/update_free". Следует отметить, что обращение к данному разделу возможно без персональных атрибутов, однако при этом обновляются только дополнительные вирусные базы для последней (новейшей) версии программы Dr.WEB.

- Каталог на локальном или сетевом диске, например, "F:\DRWEB\UPDATE";
- Сетевой каталог, например, "\\UPDATE_SERVER\DRWEB\UPDATE".

При работе подсистемы обновления с использованием прокси-сервера, требующего аутентификации, в полях *Имя пользователя прокси-сервера* и *Пароль к прокси-серверу* необходимо ввести соответствующую информацию.

Закладка «Общие». На этой закладке задаются общие настройки программы Dr.WEB для Windows 95-XP.

Переключатель [Автосохранение установок при выходе] позволяет включать или отключать автоматическое сохранение всех установок программы Dr.WEB для Windows 95-XP при окончании каждого сеанса работы.

Переключатель [Использовать установки из реестра] позволяет сохранять в системном реестре Windows текущие размеры окна программы, его расположение и т.д. и восстанавливать их при следующих запусках.

С помощью регулятора [Приоритет проверки] можно изменять системный приоритет программы Dr.WEB для Windows 95-XP. Увеличение приоритета приводит к увеличению скорости работы программы, требуя больших системных ресурсов, что приводит к замедлению работы других запущенных в системе задач. Поэтому, если Вы планируете запустить Dr.WEB для Windows 95-XP, и пока он занимается поставленной перед ним задачей, поработать с Microsoft Word, то лучше уменьшить приоритет проверки. При монопольном запуске Dr.WEB и желании получить результаты как можно скорее, целесообразно приоритет установить максимальным.

Настройка программы SpIDer

ВНИМАНИЕ! Любое изменение настроек SpIDer вступает в силу только после перезагрузки MS Windows.

Загруженный резидентный сторож SpIDer не может быть отключен или выгружен в течение всего текущего сеанса работы в MS Windows. Чтобы отключить автоматическую загрузку SpIDer в следующем сеансе работы в Windows, необходимо убрать флажок [Автозагрузка программы], расположенный во **вкладке Проверка**, и завершить работу с панелью настроек нажатием кнопки Ok.

Группа переключателей *Режим проверки «на лету»* определяет, какие именно типы файловых операций подлежат перехвату «на лету», т.е. в каких случаях сторож должен проверять объекты, к которым происходит обращение. Можно установить следующие режимы:

[Запуск и открытие] - проверка программных файлов при запуске и всех открываемых файлов;

[Создание и запись] - проверка всех создаваемых новых файлов и всех существующих файлов при их изменении, записи в них;

[Оптимальный] -

- (1) на локальных жестких дисках антивирусная проверка выполняется как в режиме "Создание и запись", т.е. только для файлов, в которые производится запись, в то время как файлы, открываемые только на чтение, в частности, при запуске программ, не проверяются. Другими словами, предполагается, что все файлы на локальных жестких дисках уже были проверены ранее, при их создании или изменении (впрочем, их все равно стоит периодически проверять, особенно при обновлении версии Dr.Web или дополнении вирусной базы);
- (2) на сетевых дисках и сменных носителях файлы проверяются всегда - при обращении к ним как на запись, так и на чтение (т.е. этот режим объединяет "Запуск и открытие" и "Создание и запись").

Замечание: перехват обращений к файлам на сетевых дисках обеспечивается только для стандартных сетевых клиентов Microsoft. Если используется другой сетевой клиент, например, Novell, то перехват обращений к файлам на сетевых дисках может не поддерживаться.

Флажок [Контроль вирусной активности] включает (выключает) специальный режим работы SpIDer, который позволяет обнаруживать и блокировать попытки вирусов, в том числе неизвестных и даже не определяемых эвристическим анализатором, заражать файлы. При обнаружении вирусной активности имеется возможность запретить выполнение вызвавшей подозрения операции записи в файл. При этом, однако, следует иметь в виду, что в случае некоторых типов резидентных вирусов файл может быть в результате разрушен.

Для просмотра результатов работы SpIDer'a в текущем сеансе предназначена **закладка Статистика**.

В поле *Проверено*: выводится общее число проверенных объектов (как файлов, так и загрузочных областей).

В поле *Инфицированных*: выводится количество объектов, инфицированных известными SpIDer'у вирусами.

В поле *Модификаций*: выводится количество объектов, инфицированных модификациями известных SpIDer'у вирусов.

В поле *Подозрительных*: выводится количество объектов, вызвавших срабатывание эвристического анализатора, т.е. подозрительных на наличие вирусов с точки зрения SpIDer'a.

В поле *Вирусных действий*: выводится число подозрительных действий, отмеченных анализатором вирусной активности. Ненулевые значения могут отражать как наличие неизвестных вирусов, так и «подозрительное» поведение ряда специфических программных приложений.

В поле *Исцелено*: указывается общее количество успешно вылеченных инфицированных объектов.

В поле *Удалено*: указывается общее количество удаленных инфицированных объектов.

В поле *Переименовано*: указывается общее количество переименованных объектов.

В поле *Перемещено*: указывается общее количество перемещенных объектов.

В поле *Запрещен доступ*: указывается общее количество объектов, в доступе к которым было отказано программой SpIDer.

Содержимое остальных закладок соответствует содержанию соответствующих закладок Dr.WEB для Windows 95-XP.

Настройка программы Планировщик DrWebWCL

После запуска Планировщика он становится активным, и признаком этого служит иконка с часами в правой части панели задач Windows (System Tray). Двойным нажатием левой кнопки мыши (или одинарным - правой) на этой иконке вызывается панель Планировщика, содержащая список заданий и меню Планировщика.

Среди настроек Планировщика при его запуске всегда включается режим автозагрузки, означающий автоматическую активизацию Планировщика при каждой перезагрузке Windows.

Если по каким-то причинам автозагрузку в следующем сеансе работы Windows требуется отключить, то нужно снять отметку в меню [Настройки | Автозагрузка программы].

Для нового задания Планировщику указывается:

- Заголовок - произвольное название задания;
- Путь - имя программы, подлежащей запуску, с полным путем;
- Параметры - набор параметров, которые должны быть переданы запускаемой программе в командной строке, если таковые требуются;
- Расписание запусков - поддерживаются следующие типы расписаний:
 - Однократно - указывается точная дата и время запуска задания;
 - Ежечасно - указывается, на какой минуте каждого часа запускать задание;
 - Еженедельно - указывается день недели и время запуска в этот день;
 - Ежемесячно - указывается число месяца и время запуска в этот день;
 - Ежегодно - указывается число, месяц и время запуска в этот день;
 - Ежедневно - указываются дни недели (в отличие от еженедельного запуска здесь их разрешается указать несколько, например, понедельник, среда, пятница) и время запуска в этот день.

Задание может быть временно выключено из обработки Планировщиком без удаления самого задания. Для этого нужно в настройках задания снять отметку в поле [Разрешить].

Замечание: Если время запуска задания по некоторому расписанию уже прошло, а задание не было реально выполнено (например, так может получиться, если компьютер был в это время выключен), то существующая реализация Планировщика всегда назначает для данного задания следующее по расписанию время запуска. Таким образом, отложенные запуски пропущенных заданий не поддерживаются.

Если при установке Dr.Web пользователь заказывает использование Планировщика, то программа установки активизирует Планировщик и предусматривает ряд типовых заданий в расписании Планировщика, но для всех заданий снимает отметку [Разрешить]. Таким образом, после установки Dr.Web пользователю следует по своим потребностям настроить типовые задания и восстановить эту отметку, или описать собственные задания.


1.2. Программный комплекс Антивирус Касперского

Антивирус Касперского OEM выполняет следующие функции /8/:

- Обнаруживает и удаляет вирусы всех типов в файлах на указанных для проверки дисках, в загрузочных секторах и оперативной памяти.
- Обнаруживает и удаляет вирусы из файлов, упакованных PKLITE, LZEXE, DIET, COM2EXE и другими утилитами сжатия.
- Обнаруживает вирусы в заархивированных файлах всех наиболее распространенных форматов (ZIP, ARJ, LHA, RAR и др.).
- Использует усовершенствованный эвристический механизм поиска неизвестных вирусов (эффективность – до 92%).

Элементы главного окна. Главное окно программы состоит из трех частей:

- список дисков (вверху);
- кнопки управления (посередине);
- открывающаяся "крышка" (внизу).


В **списке дисков** необходимо выбрать те диски, которые Вы хотите проверить на вирусы. Для этого подведите курсор мыши к требуемому диску, а затем нажмите левую клавишу. Выбранный диск будет отмечен маркером. Для пролистывания списка дисков служат специальные кнопки. Кнопки  также являются индикаторами, показывающими наличие дисков вверху или внизу списка, т.е. если будет достигнут конец списка (начало списка), то кнопка исчезнет.

Основные **кнопки управления** имеют следующие назначения:

Искать - запуск проверки на вирусы. Если программа находит вирус, то информация об этом пишется в отчет, а пользователю предлагается удалить инфицированный объект. В этом режиме программа НЕ УДАЛЯЕТ вирусы, а только их ОБНАРУЖИВАЕТ.

Лечить - проверка выбранных дисков на вирусы и попытка лечения обнаруженных инфицированных объектов. Информация обо всех инфицированных и подозрительных объектах поступает в отчет. Если программа не может вылечить объект, то она предлагает его удалить.

При поиске вирусов в режиме обнаружения (лечения) кнопка Искать (Лечить) исчезает, и вместо нее появляется кнопка Стоп, для остановки проверки на вирус.

В нижней части окна располагается панель с дополнительными кнопками управления и с информацией о программе. Она выполнена в виде **открывающейся крышки**. Чтобы открыть (закрыть) крышку, нажмите на кнопку в форме треугольника , расположенную на крышке.

Дополнительные кнопки управления имеют следующие назначения:

Отчет – открытие окна отчета;

Помощь – открытие окна помощи;

Обновить – запуск обновления антивирусных баз данных;

Монитор – запуск проверки на присутствие вирусов в реальном времени. Кнопка заблокирована, если Антивирус Касперского OEM работает в режиме мониторинга.

При нажатии на изображение логотипа, которое располагается на закрытой крышке, на экране откроется браузер с WEB-страницей компании "Лаборатория Касперского". Когда крышка открыта, можно увидеть в окне информацию о продукте (названии и дате выхода версии), количестве проверенных объектов при предыдущей проверке и дате последнего обновления антивирусных баз данных, а также о количестве вирусов, которое может быть обнаружено и вылечено с помощью Антивируса Касперского OEM.

6.2. Применение антивирусных программных комплексов

6.2.1. Программный комплекс Dr.WEB

В основном окне программы задаются объекты тестирования и действия, которые необходимо осуществлять над ними. После завершения проверки в главном окне отображаются результаты работы программы или статистика всех проведенных проверок за данный сеанс работы. Кроме этого, из главного окна доступны все дополнительные функции и настройки программы через систему меню и кнопки быстрого доступа.

Большинство элементов основного окна снабжены всплывающими короткими подсказками (hints), появляющимися при совмещении указателя мышки с соответствующим элементом окна. При этом нажатие правой кнопки мышки осуществляет доступ к расширенному контекстному файлу помощи.

Для проверки объектов на наличие вирусов необходимо выбрать устройства или их часть (каталоги, файлы), которые будет проверять Dr.WEB.

Выбранные объекты для проверки могут быть запомнены для последующего использования в качестве списка проверяемых объектов по умолчанию. Для этого служат кнопки, объединенные в функциональную группу **Выбранные пути**.

С помощью кнопки **Сохранить** можно установить текущий список объектов в качестве списка проверки по умолчанию. При следующем запуске DrWeb тот же набор объектов будет выделен для проверки.

Кнопка **Восстановить** позволяет вызвать сохраненный набор по умолчанию в любой момент времени.

Кнопка **Очистить** очищает список объектов для проверки.

Запуск проверки осуществляется с помощью кнопки, расположенной в нижней правой части основного окна. Кнопка может находиться в одном из трех состояний:

- нет выбранных объектов для проверки или идет проверка памяти, неактивна;
- нажатие на кнопку приводит к запуску процесса поиска вирусов;
- нажатие на кнопку приводит к остановке процесса поиска вирусов.

Дерево дисков. Панель выбора объектов для проверки, находящаяся в центральной части основного окна, отображает древовидную структуру имеющихся в системе устройств хранения информации:

Вы можете выбрать любое устройство левой кнопкой мышки. После выбора устройства его иконка приобретет новый вид.

Для проверки какой-либо отдельной папки (каталога) необходимо открыть структуру папок (каталогов). Для этого нужно щелкнуть левой кнопкой мышки по значку (+) слева от иконки устройства. Откроется дерево папок (каталогов) устройства и теперь можно выбрать одну или несколько папок (каталогов) с помощью щелчка левой кнопки мышки:

При включении кнопки [Показывать файлы] показываются не только папки (каталоги), но и файлы и становится возможным выбор отдельных файлов для проверки.

С помощью кнопки [Перечитать] можно обновить содержимое окна дерева дисков, например, при замене носителя или подключении новых сетевых ресурсов.

Для непосредственного задания пути к проверяемому объекту доступно окно прямого ввода, вызываемое нажатием правой кнопки мышки на панели дерева объектов. В поле ввода можно ввести полный путь к проверяемому объекту и маску (например C:\Мои документы*.doc - проверка всех документов Microsoft Word в каталоге Мои документы). С помощью кнопки [...] - просмотр можно ввести путь из окна просмотра, минуя ручной ввод.

Кнопки быстрого доступа. Под меню главного окна Dr.WEB находится ряд кнопок быстрого доступа:

[Список отчета] - переключает главное окно в режим отображения отчета о результатах тестирования;

[Дерево дисков] - переключает главное окно в режим отображения дерева дисков;

[Статистика] - переключает главное окно в режим отображения статистики результатов проведенных проверок;

[Очистить список отчета] - очищает список отчета, сформированный в результате тестирования;

[Обновить через Dr.WEB Интернет] - производит запуск программы обновления Dr.WEB через Internet;

[Настройки] - вызывает окно настроек программы;

[Выход] - завершает работу программы и закрывает главное окно.

Отчет о результатах тестирования. По завершению проверки объектов на наличие вирусов в главном окне отображаются результаты тестирования. В таблице, которая может быть раскрыта на весь экран с помощью кнопки [Список отчета], отображаются **Объект**, о котором у программы есть какая-либо информация, **Путь** к нему, **Статус** объекта (название вируса, "*Возможно <класс вируса>*") и **Действие**, произведенное программой над объектом.

Появление в колонке **Статус** сообщения типа "*Возможно <класс вируса>*" означает, что произошло срабатывание эвристического анализатора, обнаружившего подозрительные действия анализируемой программы. Это не является признаком наличия известного Dr.WEB вируса, который отображается явным определением имени вируса в колонке **Статус**, однако предупреждает пользователя о возможном наличии неизвестного вируса в объекте.

В случае, если в настройках программы установлена опция "Информировать" пользователя о наличии или подозрении на наличие вируса, после окончания тестирования колонка **Действие** будет пустой, поскольку Вы не "заказали" иных действий программы, кроме выдачи информации. Вы можете принять решение о выполнении каких-либо действий самостоятельно, выделив в таблице строчку с нужным объектом и нажав правую кнопку мышки. В появившемся меню можно выбрать необходимые действия над выделенным объектом.

Нажатие кнопки [Статистика] открывает окно вывода статистических данных текущей сессии работы программы Dr.WEB. В этом окне возможен просмотр общих результатов работы программы как в целом за сессию, так и по отдельным устройствам, присутствующим в системе. Вызов статистических данных по отдельным устройствам осуществляется с помощью соответствующих кнопок.

С помощью кнопки [Обнулить статистику] можно очистить окно статистических данных.

2.2. Программный комплекс Антивирус Касперского


Вы можете задать следующие режимы работы Антивируса Касперского OEM:

- Лечение инфицированных объектов по запросу пользователя;
- Лечение зараженных объектов в режиме мониторинга;
- Обновление антивирусных баз данных;
- Составление расписания проверок и обновлений.

Для того чтобы задать **режим лечения инфицированных объектов**, выполните следующие действия:

1. В меню **Пуск (Start)** в панели задач Windows в разделе **Программы (Programs)** выберите папку **Kaspersky Anti-Virus**;

2. В открывшемся меню выберите и запустите пункт **Kaspersky Anti-Virus Scanner**. После этого на экране откроется главное окно программы.

3. В верхней части главного окна с помощью левой кнопки мыши выберите диски, которые необходимо проверить на вирусы. Для перемещения по списку используйте специальные кнопки ().

4. Нажмите на кнопку **Лечить**. Во время проверки можно просмотреть динамически обновляемый отчет о результатах проверки, нажав на кнопку **Отчет**.

В результате все инфицированные объекты, обнаруженные программой в процессе проверки на вирусы, будут вылечены. Если лечение инфицированного объекта невозможно, то будет предложено удалить этот объект.

По окончании проверки рекомендуется просмотреть результаты проверки в отчете, нажав на кнопку **Отчет**.

Вы также можете задать режим поиска и лечения инфицированных объектов на любом диске, в любой директории и файле, *не загружая программу*.

Для того чтобы реализовать такой режим работы:

1. В панели задач Windows нажмите на кнопку **Пуск (Start)**, выберите раздел **Программы (Programs)** и запустите программу **Проводник (Windows Explorer)**.

2. Выберите в левом или правом фрейме программы любой объект(ы) (файл, директорию, диск) и нажмите на правую кнопку мыши. В открывшемся меню выберите раздел **Антивирус Касперского OEM** и в раскрывшемся списке запустите один из пунктов:

- **Лечить** – проверить объект на вирусы и при обнаружении – лечить.
- **Искать** – проверить объект на присутствие вирусов.

При обнаружении в режиме поиска или невозможности вылечить инфицированный объект в режиме лечения программа выдаст соответствующее сообщение и предложит его удалить.

Антивирус Касперского OEM позволяет также проверять и лечить инфицированные объекты при их открытии, копировании и запуске, то есть в реальном времени. Для этого предусмотрен специальный режим работы программы – **мониторинговый режим**.

Данный режим запускается автоматически сразу после установки Антивируса Касперского OEM на Ваш компьютер, на что указывает значок в панели задач Windows.

Работая в таком режиме, программа, прежде чем разрешить доступ к файлу, проверит его, а затем, в случае обнаружения вируса, выдаст на экран диалоговое окно, где предложит пользователю один из следующих способов обработки объекта:

- **Только отчет** – внести информацию об инфицированном объекте в отчет;
- **Лечить** – попытаться вылечить инфицированный объект, и, в случае неудачи, удалить;
- **Удалять объект** – удалить инфицированный объект без попытки его лечения.

Чтобы программа попыталась вылечить инфицированный объект, а в случае неудачи – удалила его:

1. Выберите способ обработки **Лечить**;
2. Нажмите на кнопку **ОК**.

Чтобы программа в режиме мониторинга пыталась лечить все инфицированные объекты, а в случае неудачи удаляла их:

1. Выберите способ обработки **Лечить**;
2. Установите флажок **Применить ко всем инфицированным объектам**;
3. Нажмите на кнопку **ОК**.

4. В открывшемся окне нажмите на кнопку **ОК**.

Обновление антивирусных баз. Для обеспечения надежной антивирусной защиты необходимо ежедневно обновлять антивирусные базы данных.


Для получения обновлений антивирусных баз предусмотрен специальный режим Антивируса Касперского OEM, который позволяет копировать антивирусные базы с WEB-сервера или FTP-сервера, а также с CD-ROM и размещать их в нужной папке так, чтобы они были доступны для работы программы.

Вы можете обновить антивирусные базы одним из следующих способов:

- Через Internet;
- Через CD-ROM.

Чтобы обновить антивирусные базы Антивируса Касперского OEM:

1. В меню **Пуск (Start)** в панели задач Windows в разделе **Программы (Programs)** выберите папку **Kaspersky Anti-Virus** и запустите программу **Kaspersky Anti-Virus Scanner**. После этого на экране откроется главное окно программы. Данное действие выполняется в том случае, если Антивирус Касперского OEM не был загружен ранее.

2. Откройте "крышку", нажав на кнопку .

3. В главном окне программы нажмите на кнопку **Обновить**.

4. В открывшемся окне выберите необходимый способ обновления антивирусных баз.

5. Нажмите на кнопку **ОК**. Процесс обновления будет отображаться на экране. После окончания обновления программа выдаст соответствующее уведомление.

Составление расписания проверок и обновления. Антивирус Касперского OEM предоставляет возможность формирования расписания проверок и обновления, в соответствии с которым программа автоматически будет производить проверку всех дисков и обновление антивирусных баз данных через Internet.


Расписание формируется из задач. Задача – это действие (последовательность действий), которое будет автоматически выполняться программой в соответствии с параметрами, заданными пользователями при ее формировании.

ВНИМАНИЕ: Во время проверки дисков на присутствие вирусов и лечения обнаруженных инфицированных объектов создать (редактировать) задачу невозможно!

Чтобы сформировать задачу:

1. В меню **Пуск (Start)** в панели задач Windows в разделе **Программы (Programs)** выберите папку **Kaspersky Anti-Virus** и запустите программу **Kaspersky Anti-Virus Scanner**. После этого на экране откроется главное окно программы.

2. С помощью правой кнопки мыши в любой части окна (кроме раздела списка дисков) вызовите динамическое меню, в котором выберите пункт **Настройка расписания задач**.

3. В открывшемся окне нажмите на кнопку .

4. В окне формирования задачи задайте значения для следующих параметров:

• **Тип задачи** – наименование типа задачи, которое Вы можете выбрать из раскрывающегося списка, содержащего следующие значения:


- *Запуск сканера* – запуск проверки на вирусы всех дисков Вашего компьютера.
- *Запуск утилиты обновления* – запуск обновления антивирусных баз через Internet.

• **Имя** – имя задачи. Обязательно задайте имя задачи, иначе она не будет создана. Если имя задачи состоит из нескольких слов, то между словами рекомендуется вставлять символ " _".

• **Периодичность** – частота выполнения задачи. Значение данного параметра задается с помощью раскрывающегося списка, содержащего следующие значения:

- *Без расписания* – не выполнять данную задачу.
- *Ежемесячно* – выполнение задачи раз в месяц. Выбрав данный вид периодичности, Вам необходимо установить значения для параметров **Число месяца** и **Время**.

- *Еженедельно* – выполнение задачи раз в неделю. Выбрав данный вид периодичности, Вам необходимо установить значения для параметров **День недели** и **Время**.
- *Ежедневно* – выполнение задачи раз в день. Выбрав данный вид периодичности, Вам необходимо установить значение для параметра **Время**.

• **Время** – время суток, когда нужно запустить выполнение задачи. Редактирование времени осуществляется с помощью стрелочек . Так, чтобы изменить время с 16:20 на 19:00, необходимо выделить сначала количество часов и увеличить его до 19, а затем выделить количество минут и уменьшить его до 00.

• **День недели** – название дня недели, когда нужно запустить задачу на выполнение. Вы можете установить значение параметра с помощью раскрывающегося списка, который доступен только в том случае, если установлено еженедельное выполнение задачи.

• **Число месяца** – число месяца, когда нужно запустить выполнение задачи. Вы можете установить значение параметра с помощью раскрывающегося списка, который доступен только в том случае, если установлено ежемесячное выполнение задачи.

Например, чтобы задать обновление антивирусных баз ежедневно в 19 часов, задайте следующие значения для параметров задачи:

1. В качестве **Типа задачи** установите **Запуск утилиты обновления**.
2. Присвойте задаче имя, например, **Ежедневное_обновление**.
3. В качестве значения параметра **Периодичность** установите **Ежедневно**.
4. В поле параметра **Время** установите значение **19:00**.
5. Нажмите на кнопку **ОК**.

В результате выполненных действий будет создана задача, которая будет выполняться программой автоматически, а именно: будет производиться автоматическое обновление антивирусных баз данных через Internet каждый день в 19 часов.

Чтобы задать проверку на вирусы всех дисков компьютера еженедельно в среду в 8 часов, задайте следующие значения для параметров задачи:

1. В качестве **Типа задачи** установите **Запуск сканера**.
2. Присвойте задаче имя, например, **Сканирование_дисков**.
3. В качестве значения параметра **Периодичность** установите **Еженедельно**.
4. В поле параметра **Время** установите значение **8:00**.
5. В качестве значения параметра **День недели** установите **среда**.
6. Нажмите на кнопку **ОК**.

ЛЗ-07. Исследование программных средств борьбы с компьютерными вирусами

Цель: Изучить и технологию использования программных средств борьбы с компьютерными вирусами. Студенты уясняют и выполняют задания ЛЗ, выполняют все работы по ним

Учебные вопросы:

- 7.1. Исследование результатов воздействия вирусов на программы в среде ОС
- 7.2. Исследование результатов работы антивирусных программ

Литература:

1. Герасименко В. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат, 1994.
2. Шураков В. Обеспечение сохранности информации в системах обработки данных. - М.: Финансы и статистика, 1985.
3. Стенг Д., Мун С. Секреты безопасности сетей. - Киев: Диалектика, 1996.

7.1. Исследование результатов воздействия компьютерных вирусов на программы в среде ОС

Некоторые проявления компьютерных вирусов и описания механизмов их работы приведены ниже.

ЗАРАЗА (1, 2)

Файлово-загрузочные вирусы. Заражают Boot-сектора дискет и системный файл IO.SYS для MS-DOS или аналогичный ему в других DOS. При загрузке с инфицированной дискеты вирусы считывают в память 5 секторов корневого каталога (root directory) загрузочного раздела жесткого диска и проверяют атрибут метки тома (Volume) у первого элемента директория. Обычно, первым элементом является системный файл IO.SYS. Если атрибут Volume установлен, то вирусы никаких действий не производят, считая что IO.SYS уже инфицирован, и передают управление оригинальному Boot-сектору флоппи-диска. Если же атрибут метки тома не установлен, то вирусы считывают в память целиком файл IO.SYS, «продвигаясь» непосредственно по цепочке FAT. Затем производят копирование системного файла в последние кластеры логического раздела. Причем вирусы очень аккуратно «просматривают» FAT для последних секторов диска, и если файл не помещается в последние 256 кластеров диска, то вирусы отказываются от дальнейшего заражения. Затем вирусы корректируют две копии FAT в соответствии с дублированием IO.SYS в последний сектор раздела. Копируют служебные поля элемента IO.SYS в третий элемент корневого оглавления. Сдвигая все оглавление с третьего элемента по 80, уничтожая, т.о., 80 элемент (файл или директорий). Устанавливают для третьего элемента (копия IO.SYS) новый начальный кластер. После чего вирусы записывают в начальный кластер первого элемента (оригинальный IO.SYS) 1024 байта своего кода. И только после этого вирусы устанавливают атрибут Volume для первого, инфицированного элемента корневого директория. Таким образом, при загрузке системы с жесткого диска, Boot-сектор активного раздела находит первый элемент в root directory IO.SYS, не обращая внимания на установленный атрибут метки тома, считывает первый кластер данного драйвера, содержащий в себе 1024 байта вирусного кода, в память и отдает ему управление. Получив управление, вирусы действуют как «обычные» Boot-вирусы – «отрезают» от памяти DOS 2 или 3 килобайта, переносят в «отрезанную» область свою копию и перехватывают INT 13h (ЗАРАЗА (1)) или INT 16h (ЗАРАЗА (2)), для заражения Boot-секторов дискет. После того как вирусы стали резидентно в памяти, они считывают в память первый кластер «файла-дублера» IO.SYS и передают ему "бразды правления". Дальше все происходит, как в незараженной системе: первый кластер отработав, находит второй кластер инфицированного файла, считывает его в память, передает ему управление и т.д. Стоит сказать о том, что зараженный файл IO.SYS, имеющий атрибут Volume, не виден стандартными средствами DOS. Т.о., "файл-дублер" необходим, практически, для маскировки и для хранения оригинального первого кластера IO.SYS. Вирусы не заражают файл IO.SYS если ак-

тивный раздел диска содержит меньше, чем 20740 (5104h) секторов, т.е. емкость диска < 10370 Кб. Опасность вирусов состоит в том, что даже при загрузке с "чистого" системного флоппи-диска и ввода команды SYS C:, вирусные коды не будут удалены с диска!!! Данная команда произведет перезапись только "файла-дублера" IO.SYS. И самое неприятное в том, что если программа SYS запишет файл на новое место на диске, то система перестанет загружаться с жесткого диска, т.к., вирусы в своем теле хранят адрес начального сектора "файла-дублера" IO.SYS. При заражении Boot-секторов флоппи диска вирусы шифруют свой код, причем расшифровщик выбирается из 12 возможных. Оригинальный Boot-сектор и свое продолжение (код, внедряемый в файл IO.SYS) вирусы "хранят" в двух последних секторах Root Directory дискеты. При загрузке системы в августе месяце ЗАРАЗА (1) выводит сообщение В BOOT СЕКТОРЕ ЗАРАЗА!

ЗАРАЗА (1) неработоспособен в 25% на процессорах 286, 386, 486 из-за ошибки при использовании конвейера. ЗАРАЗА (2) при загрузке системы в декабре издает звуковой сигнал.

A1B2.478

Опасный замещающий вирус. По окончании своей работы вирус имитирует ошибку позиционирования на текущем диске и выводит сообщение:

Seek error reading drive
Abort, Retry, Ignore, Fail?

При нажатии на клавишу "A" вирус отдает управление DOS. Содержит в начале кода текстовую строку "A1B2C3D4", которая используется, как инструкции ассемблера. При не нахождении в текущем каталоге на флоппи-диске файлов *.COM вирус, видимо, хотел бы отформатировать нулевую дорожку данной дискеты, но в данном месте имеется ошибка, и форматирование не произойдет.

A&A

Неопасный резидентный вирус. С февраля по ноябрь каждый час переставляет соседние символы на экране. Содержит текст "{A&A}".

Bingger.489

Содержит текст:

THE SMALLEST RUSSIAN VIRUS IS BINGGER THAN ENY OF THE AVENGERS

Cartier.1056

Очень опасный нерезидентный вирус. Если в текущем каталоге нет COM- файлов или они уже все инфицированы, то вирус уничтожает 50 секторов диска C: и выводит текст:

Don't panic it, I am just a virus named [Cartier]. Nice to meet you You are so dirty to get software without any payments! I don't like it So, I destroy all of your datas in the hard disk now! Feet so good!		
I wish you like that	What about a drink?	See you next time

Cat.2770

Очень опасный стелс-вирус. Заражает файл c:/command.com, если он существует. В дальнейшем заражает только .COM и .EXE-файлы, создаваемые (f.3Ch INT 21h) на дисках A: или B: при их закрытии (f.3Eh INT 21h). Т.о., в системе может быть только один зараженный файл c:/command.com. В COM-файлах либо изменяет 6 первых байт, если первая инструкция не JUMP, или 6 байт из адреса первого перехода, если первая команда - JUMP, на команды передачи управления основному вирусному коду, который находится в конце файла. 1-го числа месяца пытается уничтожить всю информацию на первом жестком диске, записывая в сектора повторяющуюся строку «Little Cat», после чего выводит текст

«Hello I am the Little Cat – lovely VIRUS!»

Maverick.Ratter

Опасный полиморфный стелс-вирус. Если значение дня равно значению месяца +1, то вирус пытается уничтожить содержимое первого жесткого диска. Не заражает программы, начинающиеся на AIDS, WEB, CHKD, SCAN.

Содержит текст «This is RATTLER v2.0. Read the Infected Voice!».

OneHalf.3544, 3570, 3577

Очень опасные полиморфные файлово-загрузочные стелс-вирусы. Используют алгоритм заражения, похожий на алгоритм CommanderBomber. Но помимо того, что "усеивают пятнами" своего кода (10 "пятен" по 10 байт) инфицированный файл, производят шифрование основного тела вируса, расположенного в конце файла. При первом запуске инфицированного файла, заражают MBR "винчестера". Оригинальный MBR и 7 секторов своего тела "прячут" в последних секторах 0 цилиндра жесткого диска. При перезагрузке компьютера, "отрезают" от доступной DOS памяти 4К, считывают в "отрезанную" верхнюю область памяти свое продолжение – 7 секторов, и перехватывают INT 13h и INT 1Ch. Контролируют с помощью INT 1Ch установку DOS'овского INT 21h, и перехватывают его. При каждой перезагрузке системы с жесткого диска последовательно, начиная с последних цилиндров, шифруют все сектора трех цилиндров на каждой головке диска. Когда вирусы находятся в памяти, они контролируют чтение секторов данных цилиндров и расшифровывают их. Если же вирусы будут удалены из MBR и памяти, то восстановление зашифрованных секторов окажется невозможным. При зашифровании половины диска вирусы выводят на экран фразу:

Dis is one half.

Press any key to continue...

После этого ожидают нажатия на любую клавишу. После чего продолжают свою дальнейшую инсталляцию в память. При попытке трассировки резидентной части вируса, предпринимают некоторые простые, но действенные меры "завешивания" системы. Содержат текстовые строки "Did you leave the room?" или "DidYou LeaveTheRoom?". Не заражают файлы с именами SCAN, CLEAN, FINDVIRU, GUARD, NOD, VSAFE, MSAV, CHKDSK, AIDS, WEB.

Sayha.DieHard

Опасный резидентный шифрованный вирус. Перехватывает INT 10h, 13h, 21h. Трассирует данные прерывания для выяснения адресов оригинальных обработчиков и для попытки "внедрения" в цепочки обработчиков прерываний. При открытии ASM-файлов записывает в них следующий текст:

```
.model small
.code
org 256
s:  push    cs
    pop     ds
    call    t
db   "Te$"
t    pop     dx
    mov     ah,9
    int     33
    mov     ah,76
    int     33
end s
```

В файлы с расширением PAS записывает:

```
bgin
wite ("Te");
```

end.

При установке графического режима (#13h 320x200 256 цветов) вирус рисует в центре экрана буквы "SW". При возникновении ошибок (переход за границу 64К при работе с DMA и данные скорректированы с использованием ECC), при попытке записи на диск, вирус пытается исправить данные ошибки! Содержит текст "SW Error", "SW DIE HARD 2".

Sayha.Watpu

Неопасный резидентный вирус. Основная часть кода вируса зашифрована, и вирус производит шифрацию своих участков во время работы. При инсталляции в память вирус трассирует INT 13h и INT 21h. Причем он может не просто перехватить INT 21h, а "вклинуться" в цепочку обработчиков INT 21h, подменяя адрес перехода в прямых или косвенных межсегментных инструкциях передачи управления (jmp far ptr ?:?, call far ptr ?:?, jmp dword ptr [?], call dword ptr [?]). В связи с этим вирус трудно обнаружить в памяти, если не проследить всю цепочку обработчиков INT 21h. 3-го и 18-го числа любого месяца, а также 15 сентября может вывести сообщение "SW Error". Вирус также перехватывает INT 16h (клавиатура).

Иногда, при нажатии на клавишу "F1", может вывести:

```
----- - -
-----ayha - -
- - - - -atpu
--- - -
```

Задание 1:

Сравнить файлы C:\V\O\V1.SYS и C:\V\M\V1.SYS,
C:\V\O\V2.SYS и C:\V\M\V2.SYS,
C:\V\O\V3.SYS и C:\V\M\V3.SYS,
C:\V\O\V4.SYS и C:\V\M\V4.SYS.

В чем различие ? (дата создания, время создания, размер и т.д.)

Результаты анализа и выводы занести в отчет.

7.2. Исследование результатов работы антивирусных программ

На жестком диске C в каталоге C:\V\O находятся четыре файла, зараженные 2-мя типами вирусов:

V1.SYS, V2.SYS, V3.SYS, V4.SYS.

Задание 2:

- 1) В каталоге C:\V создать подкаталог M (C:\V\M).
- 2) Из C:\V\O скопировать все файлы в C:\V\M (для последующего анализа).
- 3) Исследовать содержимое жесткого диска на наличие вирусов с помощью антивирусного пакета Антивирус Касперского OEM.

Результаты исследования оформить в виде отчета:

- а) Сколько проверено файлов;
 - б) Сколько найдено инфицированных файлов;
 - в) Указать какие файлы были заражены и какими вирусами;
 - г) Сколько вылечено файлов;
 - д) Вывод о результатах тестирования.
- 4) Исследовать содержимое жесткого диска на наличие вирусов с помощью антивирусного пакета DR.WEB.

Работу с программой DR.WEB выполнить в два этапа:

- 1-й этап - работа в режиме тестирования;
- 2-й этап - работа в режиме лечения каталога C:\V\M.

!!! Каталог C:\V\O лечить запрещается.

В нем должны остаться зараженные программы, которые потребуются для дальнейшей работы.

5) Сопоставить работу этих антивирусных пакетов и в отчет записать выводы по результатам сравнения.

Отчетность за занятие:

1. Результаты исследования оформить в виде отчета:

- а) Сколько проверено файлов;
- б) Сколько найдено инфицированных файлов;
- в) Указать какие файлы были заражены и какими вирусами.
- г) Сколько вылечено файлов;
- д) Вывод о результатах тестирования.

2. За 10 минут до конца занятия представить отчет преподавателю, быть готовым к ответу на вопросы по результатам исследований.

IV. Методические рекомендации руководителю по подготовке и проведению занятия:

Порядок оценки студентов при проведении занятия

В процессе занятия курсант оценивается по следующим параметрам:

- оценка за ответ на вопрос;
- оценка за добавления;
- оценка за конспект.

По результатам выставляется суммарная оценка за ответ.

Учебно-материальное обеспечение:

- Методическое руководство.
- Класс ПЭВМ, сервер Novell NetWare 3.12.
- Раздаточный материал.

Критерии оценки курсанта

Результаты контроля ответа студента на учебный вопрос определяются частными оценками "отлично", "хорошо", "удовлетворительно" и "неудовлетворительно".

Оценка "отлично" - выставляется, если студент методически грамотно изложил суть учебного вопроса, формулировки четкие и логически завершенные, выводы конкретные.

Оценка "хорошо" - выставляется, если студент правильно излагает суть учебного вопроса, но допускает отдельные неточности не принципиального характера, выводы в ответе не отличаются конкретностью.

Оценка "удовлетворительно" - выставляется, если студент правильно знает предназначение и основы функционирования программного обеспечения, без неточностей принципиального характера.

Оценка "неудовлетворительно" - выставляется, если студент не знает сути учебного вопроса, самостоятельно заявляет преподавателю о незнании или неподготовленности к ответу по данному вопросу, не обладает должной логикой мышления, а также в тех случаях, когда не выполнены условия на оценку "удовлетворительно".

Предложения преподавателя по совершенствованию содержания и методики проведения занятия.

ЛЗ-08. Построение СЗИ на основе криптографических преобразований

Цель: Изучить и практически построение систем защиты информации использующих криптографическую защиту информации. Студенты уясняют и выполняют задания ЛЗ и выполняют все работы по ним

Учебные вопросы:

- 8.1. Построение СЗИ «CryptonLITE»
- 8.2. Создание и обслуживание ключевых систем пользователя СЗИ "CryptonLITE"
- 8.3. Защита файлов и каталогов. Шифрованные логические диски

Литература:

8.1. Построение СЗИ «CryptonLITE»

Операционная система DOS фактически не имеет встроенных средств защиты. Если на компьютере хранятся конфиденциальные файлы, то будет естественным желание защитить их путем шифрования. Программа "CryptonLITE" поддерживает шифрование файлов, групп файлов, разделов и дисков в соответствии с выбранной ключевой системой и обеспечивает интерфейс пользователя при работе со средством шифрования "Криптон" /11/.

Перед отработкой практических заданий необходимо выполнить следующие действия:

- отформатировать дискету – эта дискета будет использована для записи ключевой информации;
- создать в корневом каталоге учебный рабочий каталог "WORK" и скопировать в него несколько текстовых файлов (с расширением .doc или .txt) – эти файлы будут зашифровываться/расшифровываться.

Задание 1:

1. Ознакомится с описанием комплекса, для чего в каталоге CrLite открыть и прочитать файл Read_me, и разделы 1, 2, 3.1-3.2, 3.6, 4 файла **Crtools.txt** (обратить **внимание** на выбор ключевой системы и задание ключа пользователя).
2. Запустите программу. Для этого из-под программной оболочки, поддерживающей работу в DOS (FAR, NC, VC и т.д.) наберите D:\...\CrLite\CrTools.exe и нажмите <Enter>.
3. Выполните настройку комплекса путем установки следующих параметров:
 - задание типа ключевой системы (**GK**);
 - сортировка файлов текущей директории (**по имени файла**);
 - автоудаление файлов (**не удалять**);
 - выдача информации о режиме зашифрования файла (**да**);
 - установка редактора встроенный редактор (**NC ncedit.exe**).
4. Сохранить текущие установки.

8.2. Создание и обслуживание ключевых систем пользователя СЗИ "CryptonLITE"

Для создания и обслуживания ключевых систем пользователя предназначена входящая в комплекс "CryptonLITE" программа **CrMng**.

Задание 2:

1. Ознакомится с описанием программы, для чего в каталоге CrLite открыть и прочитать файл **CrMng.txt**.
2. Выработать базовые ключи, для чего:
 - последовательно запустить программы **Cry_demo.com** и **Crnmng.exe**;
 - используя предлагаемые опции, последовательно выработать **Узел Замены** и **Главный Ключ** (использовать пароль **PSWRD**), ключи записать на подготовленную дискету.
3. Выработать пользовательские ключи, при этом, используя предлагаемые опции ввести следующие параметры:

- для ключевой системы **0** присвоить файлу с ключевой информацией имя **key0.key**, пароль - **MAXIMUM**;
- для ключевой системы **1** присвоить файлу с ключевой информацией имя **key1.key**
- для ключевой системы **4** присвоить файлу с ключевой информацией имя **key4.key**, пароль - **MEDIUM**.

ВНИМАНИЕ: при выходе из программы Crmng должна произойти перезагрузка машины, после чего перезапустить программу Cry_demo.com .

8.3. Защита файлов и каталогов. Шифрованные логические диски

Задание 3:

1. Ознакомится с описанием программы Crtools.exe, для чего в каталоге CrLite открыть и прочитать файл **Crtools.txt** (разделы 3.3-3.5).
2. Зашифровать/расшифровать тестовые файлы на базовых ключах, для чего:
 - запустите программу Crtools.exe (см п.2 задания 1);
 - зашифровать один из файлов (обратить внимание на появление нового файла с расширением **cry**);
 - удалить исходный файл;
 - убедиться в зашифровании (просмотреть зашифрованный файл с использованием встроенного редактора NC, при этом обратить особое внимание на первые две строчки зашифрованного файла);
 - расшифровать файл (обратить внимание на появление файла с исходным расширением);
 - убедиться в расшифровании файла (просмотреть его с использованием встроенного редактора NC).
3. Зашифровать/расшифровать тестовые файлы на пользовательских ключах, для чего:
 - повторить действия, изложенные п. 2, используя для зашифрования другого файла Главный ключ, Пароль (MAXIMUM) и Ключ пользователя (key0.key);
 - повторить действия, изложенные п. 2, используя для зашифрования другого файла Главный ключ и Ключ пользователя (key1.key);
 - повторить действия, изложенные п. 2, используя для зашифрования другого файла Пароль (MEDIUM) и Ключ пользователя (key4.key).
4. Просмотреть и сравнить первые строки файлов, зашифрованных на разных ключевых системах.

Задание 4:

1. Зашифровать/расшифровать тестовые файлы на пользовательском ключе с выбранной ключевой системой Главный Ключ и Ключ Пользователя с изменением Главного Ключа, для чего:
 - с помощью программы Crmng.exe создайте новый Главный Ключ (обратите на появление файла **gk_old.db3**);
 - вводите новый Главный ключ в средство шифрования;
 - перешифруйте пользовательский ключ (**key1.key**) на новом Главном Ключе;
 - уничтожьте на ключ-диске старый Главный Ключ;
 - повторить действия, изложенные п. 2 задания 3.
2. Просмотреть файлы, зашифрованные на новом Главном Ключе, сделать выводы.

Задание 5:

1. Зашифровать/расшифровать гибкий магнитный диск на пользовательском ключе с выбранной ключевой системой Главный Ключ и Ключ Пользователя, для чего:
 - установите в дисковод подлежащую зашифрованию дискету;
 - используя предлагаемые опции, зашифровать диск на пользовательском ключе key1.key;
 - просмотреть содержание зашифрованного диска;
 - расшифруйте диск аналогично процедуре зашифрования диска.

2. Перешифруйте диск на новом пользовательском ключе `key0.key` аналогично процедуре зашифрования. **ВНИМАНИЕ:** старый и новый ключи должны располагаться в одной директории.

3. Просмотреть содержание зашифрованного диска на новом ключе сравнить шифрование на разных ключевых системах, сделать выводы.

ЛЗ-09. Исследование уязвимостей программных средств криптографической защиты

Цель: Изучить и опробовать технологию исследования уязвимостей программных средств криптографической защиты. Студенты уясняют и выполняют задания ЛЗ и выполняют все работы по ним

Учебные вопросы:

- 9.1. Исследование временной стойкости криптосистемы архиватора WinZip
- 9.2. Исследование временной стойкости криптосистемы текстового редактора MS Word

Литература:

1. Герасименко В. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат, 1994.
2. Шураков В. Обеспечение сохранности информации в системах обработки данных. - М.: Финансы и статистика, 1985.
3. Стенг Д., Мун С. Секреты безопасности сетей. - Киев: Диалектика, 1996.

9.1. Исследование временной стойкости криптосистемы архиватора WinZip

Файлы ZIP имеют достаточно сильный алгоритм шифрования. Пароль не сохраняется где-нибудь в архиве, защищенном паролем. Архиватор конвертирует (преобразовывает) пароль, который вы ввели в три 32-разрядных ключа шифрования, и затем использует их, чтобы зашифровать целый архив. Таким образом, если мы будем пробовать комбинации всех возможных ключей, то полная сложность атаки - 2^{96} . Это действительно много – даже с использованием всех компьютеров в мире, невозможно перебрать все ключи. Однако, этот алгоритм не столь силен как DES, RSA, IDEA и подобные.

То, что многие криптосистемы не ограничивают минимальную длину пароля, из которого формируется ключ, как раз и приводит к успеху атак перебором не ключей, а паролей.

Программа Advanced ZIP Password Recovery (Продвинутое Восстановление Пароля ZIP, или просто AZPR) может использоваться, чтобы восстановить потерянный пароль для архива ZIP. В настоящее время, не имеется никакого известного метода извлечь пароль из сжатого файла; так что единственные доступные методы - "решение в лоб" – атака типа полный перебор и атака по словарю /12/.

Атака по словарю. Эта атака наиболее эффективна, поэтому пробуйте сначала ее.

Просто выберите желательный файл словаря. Кроме того, Вы можете выбирать мутации опции Smart или Пробовать все возможные верхние\нижние комбинации случаев - это может действительно помогать, если вы не уверены относительно регистра, в котором пароль был напечатан. Например, предположим, что следующее слово в словаре - «password». Со второй опцией, программа будет пробовать все возможные комбинации, подобно:

```
passworD
passwoRd
passwoRD
passwOrd
...
PASSWORD
PASSWORD
```

Кроме того, если Вы знаете "структуру" пароля (например, символы в некоторых позициях), рекомендуется, чтобы Вы создали ваш собственный словарь.

Генератор пароля может также помогать, если Вы "почти" помните пароль. Вы могли бы пропустить один или два символа, или напечатать дополнительный, или только пропустить несколько символов - некоторые генераторы позволяют видоизменять пароль и могут сохранять все подобные.

Когда все опции выбраны, все, что Вы должны делать это нажать кнопку Start на инструментальной панели и ждать. В течение атаки, вы будете видеть состояние программы - число проверенных паролей, прошедшее и оцененное время и т.д.

Атака типа полный перебор. Если Вы понятия не имеете, какой длины пароль и какие символы он может содержать, выполните сначала атаку по словарю.

Если это терпит неудачу, попробуйте решение "в лоб" - атаку типа полный перебор со следующими опциями (набор символов и диапазон длины пароля):

Символы	Длина	Пароли	Время
Весь печатаемый	1-5	7,820,126,720	65 минут
Цифры, маленькие	6	62,523,502,592	9 часов
Цифры, маленькие символы, пробел	7	94,931,877,888	13 часов
Цифры, заглавные буквы, пробел	7	94,931,877,888	13 часов
Цифры	8-11	111,100,002,304	15,5 часов
Маленькие символы, пробел	8	282,429,521,920	1,5 дня
Заглавные буквы, пробел	8	282,429,521,920	1,5 дня

Третий столбец показывает общее количество возможных комбинаций паролей (с данным набором символов и длины пароля); и последний столбец показывает максимальное время требуемый для восстановления пароля, в предположении, что скорость является 2,000,000 паролей в секунду.

Когда пароль найден, программа показывает это, а также число паролей, которые были проверены и скорость программы.

Последняя строка отображает пароль в шестнадцатеричной форме, что могло бы быть полезно, если пароль, например, содержит некоторые неанглийские символы, которые не могут быть отображены правильно в вашей системе.

Если все возможные пароли в данном диапазоне были испытаны без успеха выдается сообщение «пароль не найден».

Если Вы остановили восстановление, нажимая кнопку "Stop", текущий шаг сохранен в поле "Start from". Теперь Вы можете нажимать кнопку "Start" снова. Восстановление будет продолжено от этого шага.

Введите в программу, какие символы использовались в пароле. Вы можете выбирать из всех заглавных букв, всех маленьких символов, всех цифр, всех специальных символов и пробела; или только весь печатаемый (включает все выше). Специальные символы: ! @#\$%^&*()_+ -= <> ,./?[]{} ~:;`|"\' \

Длина пароля - это одна из наиболее важных опций, воздействующих на время проверки. Вы можете проверять все 4-символьные (и короче) пароли за несколько минут; но для более длинных паролей, Вы должны иметь терпение и-или некоторое знание относительно пароля (включая набор символов, который использовался, или даже лучше - маску).

Если минимальная и максимальная длина - не та же самая, программа пробует сначала более короткие пароли. Например, если Вы устанавливаете minimum=3 и maximum=7, программа начнется с 3-символьных паролей, затем будет пробовать 4-символьные и так далее - до 7. В то время как AZPR выполняется, она показывает текущую длину пароля, также текущий пароль, среднюю скорость, прошедшее и остающееся время и обработанное число паролей. Вся эта информация кроме средней скорости и прошедшего времени, которые являются глобальными, связана только с текущей длиной.

Обратите внимание, что в незарегистрированной версии AZPR, максимальная длина ограничена 5. Однако не следует ожидать восстановления паролей, которые содержат 12 или большее количество неизвестных символов в разумное время.

Вы можете определять ваш собственный набор символов. Только отметьте переключатель "Набор пользователя", и нажмите на "Определите набор символов" (направо от опции). Во входном окне, введите все символы вашего диапазона пароля; например: если Вы помните, что ваш пароль был введен в основании клавиатуры (" zxcv ... ") - ваш диапазон пароля должен быть " zxcvbnm,. / " (или в заглавных буквах: " ZXCVBNM <>? "). Вы можете также определять

оба из них: " zxcvbnm, ./ZXCVBNM < >? ". Кроме того, Вы можете загружать и сохранять заказной набор, или комбинировать их, используя кнопку "Добавляют набор от файла ...".

Атака с известным открытым текстом. Один из путей ломающий защиту ZIP использует атаку с известным открытым текстом.

Зашифровав файл, созданный ZIP архиватором, и тем же самым файлом в незашифрованной форме, мы можем делать некоторые вычисления и восстанавливать (отыскивать) ключи шифрования. Обычно, архив ZIP содержит несколько файлов, и все из них имеют тот же самый пароль (и следовательно ключи шифрования). Это означает, что, если мы получим ключи шифрования для одного из этих файлов, мы будем способны раскрыть все другие! И кроме того, не будет требоваться так много времени, как при попытке всех возможных комбинаций ключей шифрования. Чтобы выполнять атаку с известным открытым текстом все, в чем Вы нуждаетесь - один файл от архива, сжатого тем же самым архиватором и тем же самым методом как зашифрованные.

Имеются две стадии атаки "открытого текста", плюс два добавления поиска пароля (обратите внимание, что оценки времени даны для Intel Celeron 366 MHz):

1. Цикл сокращения ключей. В этой стадии, AZPR нуждается приблизительно в 34 мегабайтах (виртуальной) памяти. Этот цикл берет от одной до двух - трех минут (в зависимости от размера открытого текста). Но если Вы не имеете достаточно физической памяти, может требоваться немного большее количество времени. После этой стадии, AZPR освободит большинство памяти и будет работать только с 2-4 мегабайтами. Также обратите внимание, что время, требуемое, чтобы завершить эту стадию не может быть оценено, так сначала несколько минут индикатор хода работы будет в 0%, а затем будет быстро увеличиваться.

2. Поиск ключей соответствия. Это - основная стадия атаки "открытого текста". Теперь Вы можете видеть, сколько времени Вам необходимо в самом плохом случае для восстановления архива. В зависимости от размера открытого текста, эта стадия может длиться от 5 минут до нескольких часов.

Атака на частичный файл. Иногда архив ZIP тот, который не защищен паролем и второй, могут отличаться по размеру. Например, WinZip может создавать такие, если исходный файл почти не может быть сжат. Однако, Вы можете исполнять, атаку открытого текста на такие файлы, для этого нужно сохранить в защищенном паролем архиве только один файл (который будет атакован); (конечно, сначала зарезервируйте ваши первоначальные файлы). И также сохраните только один файл в архиве "открытого текста". Выполните атаку, AZPR будет просить о подтверждении "частичного" нападения. Нажмите Да, и выберите число байтов, чтобы использовать открытый текст. Поскольку мы не знаем, сколько байтов могут быть использованы, хороший подход - запустить с 1-3Kb (в большинстве случаев это является достаточным) и уменьшать это количество, если AZPR не будет способен найти ключи шифрования.

Файл "Открытого текста" должен быть по крайней мере длиной 16 байтов и Вы нуждаетесь приблизительно в 48 мегабайтах ОЗУ.

Имеются результаты (эталонные тесты) атаки "известный открытый текст" для различных файлов (на Intel Celeron 366MHz с 64МБ ОЗУ).

Размер файла (байты)	Стадия #1 Время	Стадия #2 Время
16	20s	2d 12h
32	33s	8h 30m
64	38s	3h 30m
128	45s	1h 45m
256	52s	42m
512	52s	20m
1024	52s	8m
2048	1m 5s	5m 30s
4096	1m 5s	4m
8192	1m 14s	4m
16384	1m 30s	4m
32768	2m 10s	4m

Описание лабораторной установки. Программа AZPR имеет удобный интерфейс пользователя и следующие возможности:

- Программа очень быстрая: приблизительно два миллиона паролей в секунду на Pentium II.
- Программа может работать с архивом, содержащим только один зашифрованный файл. Поддержан самоизвлекающийся архив.
- Программа настраиваема: Вы можете менять длину пароля (или диапазон длины), набор символов использоваться, чтобы генерировать пароли, и пару других опций.
- Вы можете выбирать заказной набор символов для поиска решения "в лоб" (поддержаны неанглийские символы).
- Доступна атака по словарю (с мутациями слова). Доступна атака типа полный перебор, решение "в лоб" с маской. Доступна атака с известным открытым текстом.
- Максимальная длина пароля не ограничена (в зарегистрированной версии).
- Вы можете прерывать программу в любое время, и позже перезапустить от того же самого пункта (точки).
- Программа может работать в фоновом режиме, используя процессор только, когда он находится в неактивном состоянии.

Задание 1:

1. В каталоге C:\LR65 создать текстовый файл text1.txt; с помощью архиватора WinZip создать архивы закрытые паролями соответственно:

text1.zip – 12345
 text2.zip – 1234z
 text3.zip – 123Zz
 text4.zip – 12\$Zz
 text5.zip – krypton

2. Выполнить атаку по словарю с каждым архивом.

3. Выполнить атаку типа полный перебор. Построить таблицу зависимости времени вскрытия пароля от длины пароля n , (при $n = 2, 3, 4, 5$) и множества допустимых символов s (при $s = 10, 30, 62, 93$).

4. Построить таблицу зависимости времени вскрытия пароля от множества допустимых символов s , при $s = 10, 30, 40, 52, 62, 82, 93$ (при $n = 5$).

5. Выполнить атаку типа полный перебор с маской «???z».

6. Сделать выводы о методе реализации криптографического средства, ключевой системы, о методике выбора паролей.

7. Результаты исследований, таблицы, и выводы занести в отчет.

Задание 2:

1. В каталоге C:\LR65 создать текстовый файл text2.txt; С помощью архиватора WinZip создать архив tzip.zip из двух файлов text1.txt и text2.txt закрытый паролем.

2. Подготовить незашифрованный файл tnzip.zip из text1.txt, который также существует в защищенном паролем архиве. Сжать его с тем же самым методом и тем же самым ZIP, как в зашифрованном архиве. Обратите внимание, что это строго необходимо, потому что AZPR проверяет размеры файла и контрольные суммы файлов.

3. Запустите AZPR, выберите зашифрованный архив, затем выберите нападение "plaintext" и обзор для архива с незашифрованным файлом. После этого AZPR проверит файлы, и если они соответствуют, атака начата.

4. Сделать выводы об уязвимости, методе реализации криптографического средства, ключевой системы.

5. Результаты исследований, таблицы, и выводы занести в отчет.

9.2. Исследование временной стойкости криптосистемы текстового редактора MS Word

Не секрет, что программный пакет Microsoft Office является самым популярным и наиболее используемым для подготовки документов. При работе с приложениями MS Office возника-

ет проблема обеспечения конфиденциальности информации, хранящейся в документах. К сожалению не все способы защиты, реализованные в этом пакете, позволяют надежно защитить информацию.

Защита документов Microsoft Word возможна тремя способами:

- защита документа от записи;
- защита документа от изменений;
- пароль на документ.

Защита документа от записи является самым слабым. Пароль защиты записи хранится в документе в чистом виде. Можно даже поискать его любым hex-редактором. Хранится он в unicode. Пароль даже не удосужились захешировать. Снять эту "защиту" можно изменением одного бита в документе.

Криптостойкость способа защиты документа от изменений не намного отличается от предыдущего пароля. Отличие только в том, что этот пароль хешируется. Длина хеша - 32 бита. Можно либо заменить хеш на заранее известный, либо вычислить первый подходящий пароль. Понятно, что для такой длины хеша подходящих паролей может быть несколько.

Из всех существующих способов защиты документов Word пароль на документ является самым стойким. При установке этого пароля документ шифруется по симметричному алгоритму RC4. В документе хранится зашифрованный хеш пароля, используемый при проверке. Единственный способ нахождения пароля - перебор. Однако экспортные ограничения на криптоалгоритмы значительно снижают криптостойкость этой защиты. Ключ, используемый при шифровании RC4, имеет длину 40 бит. Если перебирать не пароли, а ключи, искомым ключ можно найти за 30 дней на P-II 350. В документах Office 95 используется более простой способ шифрования, который позволяет найти пароль любой длины почти мгновенно.

Advanced Office 97 Password Recovery (Продвинутое Восстановление Пароля Office 97, или просто АО97PR) - программа для восстановления потерянных паролей к документам Microsoft Office 97/2000. Она позволяет находить пароли к документам Word 97, Excel 97 и любой 32-битной версии MS Access. Пароли к Word и Excel находятся методами прямого перебора, перебора по маске и по словарю. Перебор можно прервать и продолжить в любое время. Пароли для MS Access, пароли защиты записи и книг/листов MS Excel находится прямым декодированием. Возможно сохранение всех опций программы в файле проекта. В версии 1.22 поддерживаются все документы Office 2000 /13/.

Алгоритм вскрытия паролей с помощью АО97PR аналогичен алгоритму работы с AZPR:

- 1) если вы понятия не имеете, какой длины пароль и какие символы он может содержать, выполните сначала атаку по словарю;
- 2) если вы уже знаете некоторые символы в пароле, то для уменьшения общего числа паролей, которые нужно проверять, определите маску и выполните атаку перебора по маске. В данной версии, вы можете установить маску только для фиксированной длины паролей;
- 3) если первые два этапа не принесли результата, пробуйте решение "в лоб" - атаку типа прямой перебор со следующими опциями (набор символов и диапазон длины пароля):

Символы	Длина	Пароли	Время
Весь печатаемый	1...4	82,317,120	30 минут
Цифры, маленькие (заглавные), пробел	5	999,436,544	5,5 часов
Цифры, маленькие символы, пробел	6	2,565,726,464	14 часов
Цифры, заглавные буквы, пробел	6	2,565,726,464	14 часов
Маленькие символы, пробел	7	10,460,352,512	~60 часов
Заглавные буквы, пробел	7	10,460,352,512	~60 часов
Цифры	7...10	11,109,999,616	~60 часов

Третий столбец показывает общее количество возможных комбинаций паролей (с данным набором символов и длины пароля), а последний столбец показывает максимальное время требуемый для восстановления пароля, в предположении, что скорость является 50,000 паролей в секунду (для Pentium II).

Задание 3:

1. В каталоге C:\LR65 с помощью текстового редактора MS Word создать текстовые файлы закрытые паролями соответственно:

text1.doc – 99999
text2.doc – 9999z
text3.doc – 999Zz
text4.doc – 99\$Zz
text5.doc – vampire

2. Выполнить атаку по словарю с каждым архивом.

3. Выполнить каждую атаку типа полный перебор до конца. Построить таблицу зависимости времени вскрытия пароля от длины пароля n , (при $n = 2, 3, 4, 5$) и множества допустимых символов $s = 26$.

4. Построить таблицу зависимости времени вскрытия пароля от множества допустимых символов s , при $s = 10, 30, 40, 62, 82, 93$ (при $n = 4$).

5. Выполнить атаку типа полный перебор с маской «???z».

6. Сделать выводы об уязвимости, методе реализации криптографического средства, ключевой системы, о методике выбора паролей.

7. Результаты исследований, таблицы, и выводы занести в отчет.

ЛЗ-10. Аппаратные средства опознавания пользователей

Цель: Изучить и опробовать аппаратные средства опознавания пользователей. Студенты уясняют и выполняют задания ЛЗ и выполняют все работы по ним

Учебные вопросы:

- 10.1. Построение аппаратных средств СЗИ (электронный замок "Соболь")
- 10.2. Управление пользователями в СЗИ (электронный замок "Соболь")

Литература:

1. Герасименко В. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат, 1994.
2. Шураков В. Обеспечение сохранности информации в системах обработки данных. - М.: Финансы и статистика, 1985.
3. Стенг Д., Мун С. Секреты безопасности сетей. - Киев: Диалектика, 1996.

10.1. Построение аппаратных средств СЗИ (электронный замок "Соболь")

Система *Электронный замок "Соболь"* (далее по тексту - *Электронный замок*) предназначена для организации защиты компьютера от входа посторонних пользователей. Под посторонними пользователями понимаются все лица, не зарегистрированные в системе *Электронный замок* как пользователи данного компьютера /14/.

Система *Электронный замок* обеспечивает:

- регистрацию пользователей компьютера и назначение им персональных идентификаторов и паролей на вход в систему;
- запрос персонального идентификатора и пароля пользователя при загрузке компьютера;
- возможность блокирования входа в систему зарегистрированного пользователя;
- ведение системного журнала, в котором производится регистрация событий, имеющих отношение к безопасности системы;
- контроль целостности файлов на жестком диске;
- контроль целостности физических секторов жесткого диска;
- аппаратную защиту от несанкционированной загрузки операционной системы с гибкого диска и CD-ROM диска.

Система *Электронный замок* включает в свой состав следующие средства защиты компьютера:

- **механизм идентификации и аутентификации** пользователей, обеспечивающий проверку полномочий пользователя на вход при попытке входа в систему;
- **подсистему контроля целостности**, обеспечивающую контроль целостности файлов на жестком диске и физических секторов жесткого диска;
- **подсистему запрета загрузки со съемных носителей**, обеспечивающую запрет загрузки операционной системы с гибкого диска и CD ROM диска.

Механизм идентификации и аутентификации

Идентификация (распознавание) и *аутентификация* (проверка подлинности) осуществляется при каждом входе пользователя в систему. При загрузке компьютера система *Электронный замок* запрашивает у пользователя его персональный идентификатор и пароль. Осуществляется проверка наличия в системе зарегистрированного пользователя, которому присвоен предъявленный при входе персональный идентификатор. Если предъявлен персональный идентификатор, не зарегистрированный в системе (не принадлежащий ни одному пользователю компьютера), вход в систему пользователя запрещается, а в системном журнале регистрируется попытка несанкционированного доступа к компьютеру.

Аутентификация пользователя осуществляется после его идентификации для подтверждения права использовать предъявленный персональный идентификатор для входа в систему. При аутентификации пользователя осуществляется проверка правильности указанного им пароля. В системе *Электронный замок* поддерживается работа с паролями длиной до 16 символов. Вводимый пароль не отображается на экране компьютера. Если пароль указан неверно (не соответствует предъявленному идентификатору), вход пользователя в систему запрещается, а в системном журнале регистрируется попытка несанкционированного доступа к компьютеру.

Служебная информация о регистрации пользователя (имя, номер присвоенного персонального идентификатора и т.д.) хранится в ОЗУ платы *Электронный замок*.

Подсистема контроля целостности. Подсистема контроля целостности предназначена для контроля целостности файлов и секторов жесткого диска, с целью убедиться, что эти файлы и сектора не были модифицированы. Для этого вычисляются некоторые контрольные значения проверяемых объектов и сравниваются с их заранее рассчитанными эталонными значениями. Подсистема включает в себя следующие компоненты:

- модуль контроля целостности;
- программу формирования шаблонов для контроля целостности;
- задания на контроль целостности.

Модуль контроля целостности является программным модулем *ROM BIOS* платы *Электронный замок*. Он обеспечивает расчет эталонных значений контрольных сумм проверяемых файлов и секторов жесткого диска, сохранение полученных контрольных сумм в файлах заданий на проверку контроля целостности и проверку контрольных сумм проверяемых объектов при каждой загрузке компьютера. Контрольные суммы рассчитываются по алгоритму ГОСТ 28147-89 в режиме имитоприставки. При проверке контрольных сумм файлов и секторов осуществляет сравнение текущих значений контрольных сумм с эталонными (заранее вычисленными) значениями контрольных сумм проверяемых объектов, хранящихся в соответствующих файлах заданий на проверку контроля целостности.

Программа формирования шаблонов для контроля целостности является дополнительным программным обеспечением, поставляемым вместе с платой *Электронный замок* и устанавливаемым на жесткий диск компьютера. Эта программа позволяет определить перечень файлов и физических секторов жестких дисков, подлежащих контролю, и создать шаблоны заданий на контроль целостности, содержащие полный путь к каждому контролируемому файлу и координаты каждого контролируемого сектора.

Задания на контроль целостности содержат информацию о местоположении контролируемых файлов на жестком диске (полный путь к ним), координаты контролируемых секторов, а также значения контрольных сумм для каждого файла или сектора.

Подсистема запрета загрузки со съемных носителей. Подсистема запрета загрузки с гибкого диска и CD ROM диска обеспечивает запрет загрузки операционной системы с этих съемных носителей для всех пользователей компьютера, кроме администратора.

Запрет загрузки осуществляется путем блокирования доступа к устройству чтения гибких дисков (НГМД) и устройству чтения CD ROM дисков при запуске и загрузке компьютера. После того как загрузка компьютера успешно завершена, доступ к этим устройствам восстанавливается специальной программой-драйвером, входящей в состав программного обеспечения системы *Электронный замок*.

Требования к оборудованию и программному обеспечению. Система *Электронный замок* может быть установлена только на компьютеры, оснащенные процессорами семейства *INTEL X86* (или совместимыми с ними), начиная с процессора *i386* и выше.

Система *Электронный замок* поддерживает работу со следующими модификациями персональных идентификаторов *Touch Memory*: DS1992, DS1993, DS1994, DS1995, DS1996.

Для подключения платы *Электронный замок*, системная плата компьютера должна быть оснащена системной шиной *ISA*, и должен быть в наличии хотя бы один свободный разъем этой шины.

Не допускается использование системным *BIOS* режима Shadow Memory для адресного пространства, в котором будет размещаться расширение *BIOS*, содержащееся в ПЗУ платы *Электронный замок*.

Работоспособность системы *Электронный замок* не зависит от типа используемой операционной системы, поэтому она может быть установлена на компьютеры, работающие под управлением различных операционных систем.

Подсистема контроля целостности и подсистема запрета загрузки со съемных носителей, являющиеся дополнительными компонентами системы *Электронный замок*, включают в свой состав программные компоненты. Успешная работа этих компонент зависит от операционной системы, установленной на компьютер. В настоящее время комплект поставки системы *Электронный замок* включает в свой состав программные компоненты этих подсистем, функционирующие под управлением следующих операционных систем:

- *MS DOS* версий 5.0-6.22;
- операционных систем семейства *Windows'9x* (*Windows 95*, *OSR2*, *Windows 98*) с файловой системой FAT16 или FAT32;
- *Windows NT* версий 3.51 и 4.0 с файловой системой NTFS.

10.2. Управление пользователями в СЗИ (электронный замок "Соболь")

Установка системы на компьютер. Установка системы *Электронный замок* на компьютер осуществляется в следующем порядке:

1) Производится установка программного обеспечения и настройка подсистемы контроля целостности, если это необходимо. В результате установки программного обеспечения в состав меню [Программы] будет добавлено подменю [Соболь], содержащее пункт [Программа подготовки шаблонов].

2) Плата *Электронный замок* подготавливается к работе, переключается в режим инициализации и помещается в свободный разъем системной шины *ISA* компьютера.

При подготовке платы *Электронный замок* к работе определяются следующие основные параметры ее работы:

- адрес порта ввода/вывода, который будет использоваться при считывании информации из памяти персонального идентификатора и записи информации в эту память согласно таблице 11.1.

- адрес *ROM BIOS*, начиная с которого в памяти компьютера будет размещаться расширение *BIOS*, содержащееся в ПЗУ платы согласно таблице 11.2.

Определив параметры работы платы *Электронный замок*, переключите ее в режим инициализации, сняв перемычки, установленные на контактах **SW7-SW8**.

Таблица 11.1

Адрес порта ввода / вывода	Положение перемычек		
	SW1	SW2	SW3
100	+	+	+
110	-	+	+
120	+	-	+
140	-	-	+
200	+	+	-
210	-	+	-
220	+	-	-
240	-	-	-

+ - перемычка установлена (контакты замкнуты)
 - - перемычка снята (контакты разомкнуты)

Таблица 11.2

Начальный адрес ROM BIOS	Положение перемычек		
	SW4	SW5	SW6

Начальный адрес ROM BIOS	Положение перемычек		
	SW4	SW5	SW6
C800	+	+	+
CC00	-	+	+
D000	+	-	-
D400	-	-	-
D800	+	+	-
DC00	-	+	-
E000			
E400			

+ - перемычка установлена (контакты замкнуты)

- - перемычка снята (контакты разомкнуты)

Затем установите плату *Электронный замок* в компьютер. Для этого:

- выключите компьютер (если он включен);
- вскройте корпус компьютера;
- выберите свободный слот системной шины *ISA* (разъем для плат расширения) и аккуратно вставьте в него плату *Электронный замок*;
- закройте корпус компьютера;
- подсоедините штекер считывателя (входящего в комплект поставки) к разъему платы *Электронный замок*, расположенному на задней панели системного блока, и закрепите штекер крепежными винтами.

3) Выполняется процедура инициализации системы *Электронный замок*.

Включите питание компьютера. На экране появится изображение. В нижней строке экрана (называемой **Строка сообщений**) отображаются сообщения, выдаваемые системой *Электронный замок*, а также дополнительная информация о выполняемом действии.

При загрузке системы *Электронный замок* в режиме инициализации производится тестирование правильности работы датчика случайных чисел (ДСЧ) платы *Электронный замок*, которое заключается в проверке равномерности распределения случайных чисел, генерируемых датчиком. При этом в **Строке сообщений** отображается соответствующее сообщение. Если тестирование ДСЧ завершено успешно (получен положительный результат), инициализация системы *Электронный замок* будет продолжена, и на экране появится диалог определения общих параметров работы системы *Электронный замок*.

Эти параметры определяют настройки системы, являющиеся общими для всех пользователей компьютера, и могут быть в дальнейшем изменены.

Параметр **“Минимальная длина пароля пользователя”** определяет минимальную длину пароля пользователя в символах (параметр может принимать значения от 0 до 9; “0” означает - разрешено использовать пустые пароли). Пользователю нельзя назначить пароль, число символов в котором меньше числа, заданного этим параметром.

Параметр **“Предельное число неудачных входов пользователя”** определяет, сколько раз пользователь может допустить ошибку при входе в систему, указав неверный пароль (параметр может принимать значения от 1 до 65535). Если число неудачных входов пользователя в систему превысило число, заданное этим параметром, вход пользователя в систему будет блокирован.

Параметр **“Плата функционирует в автономном режиме”** определяет режим доступа любых внешних программ к области ОЗУ платы *Электронный замок*, в которой хранятся регистрационные записи системного журнала. (Этот параметр оказывает влияние на работу системы только в том случае, если *Электронный замок* используется совместно с другими системами защиты, например *Secret Net*.)

Параметр **“Показ статистики пользователю”** позволяет разрешить или запретить вывод на экран при входе пользователя в систему информационного окна, содержащего сведения о его работе.

Параметр **“Тестировать ДСЧ для пользователя”** позволяет включить или отключить тестирование правильности работы датчика случайных чисел (ДСЧ) платы *Электронный замок*, осуществляющееся при входе пользователей в систему.

Параметр **“Контролировать целостность файлов”** позволяет включить или выключить контроль целостности объектов, осуществляющийся при загрузке пользователем операционной системы.

Внесите необходимые изменения и для продолжения процедуры инициализации нажмите клавишу *<Esc>*.

В появившемся окне выберите первичный вариант регистрации администратора.

На экране появится запрос пароля администратора.

При определении нового пароля необходимо соблюдать следующие правила:

- пароль может содержать только латинские символы, цифры и служебные символы;
- разрешается использовать различные регистры клавиатуры (например, “Dog” или “dog”); при этом нужно помнить, что заглавные и прописные буквы воспринимаются как различные (“Dog” и “dog” считаются разными паролями);
- длина пароля (в символах) не может быть меньше числа, заданного общим параметром **“Минимальная длина пароля пользователя”** и не может превышать 16-ти символов.

Введите с клавиатуры пароль в поле **“Введите ... пароль :”**. Завершите ввод, нажав клавишу *<Enter>*. В окне подтверждения повторно введите тот же пароль.

Если оба значения пароля совпали, то на экране появится запрос, персонального идентификатора. Плотнo прислоните к считывателю персональный идентификатор, присваиваемый администратору. При неуспешном чтении информации из идентификатора или записи информации в идентификатор в **Строке сообщений** появится сообщение об ошибке. В этом случае повторно прислоните идентификатор к считывателю.

При *первичной* регистрации администратора производится запись служебной информации в предъявленный идентификатор.

После того как администратору присвоен персональный идентификатор, на запрос создать резервную копию идентификатора администратора ответьте «Нет». После этого на экране появляется сообщение о завершении инициализации системы защиты.

4) Плата *Электронный замок* переключается в режим обычной работы и помещается в компьютер. При этом если это необходимо, производится подключение интерфейсных кабелей, обеспечивающих работу подсистемы запрета загрузки со съемных носителей, к устройствам чтения гибких дисков и CD ROM дисков и к плате *Электронный замок*.

Чтобы переключить плату *Электронный замок* в обычный режим работы, выполните следующие действия:

- выключите компьютер (если он включен);
- вскройте корпус компьютера;
- отсоедините штекер считывателя от разъема платы *Электронный замок*, расположенного на задней панели системного блока, предварительно отвернув крепежные винты;
- аккуратно выньте плату *Электронный замок* из разъема системной шины *ISA*;
- установите перемычки на контакты **SW7-SW8** платы;
- если Вы предполагаете использовать подсистему запрета загрузки со съемных носителей, подключите интерфейсные кабели, обеспечивающие работу этой подсистемы, к устройствам чтения гибких дисков и CD ROM дисков и к плате *Электронный замок*;
- аккуратно вставьте плату в разъем системной шины *ISA*;
- закройте корпус компьютера;
- подсоедините штекер считывателя к разъему платы, расположенному на задней панели системного блока, и закрепите штекер крепежными винтами.

Выполнив все указанные действия, включите компьютер и перейдите к настройке системы *Электронный замок*.

Настройка и эксплуатация системы. После того как система *Электронный замок* установлена на компьютер, необходимо:

- определить общие параметры работы системы защиты;
- зарегистрировать в системе защиты пользователей, допущенных к работе на данном компьютере;
- (при необходимости) настроить подсистему контроля целостности.

При входе в систему, после предъявления полномочий администратора, на экране появляется информационное окно. Нажмите любую клавишу, чтобы продолжить работу, и на экране появится меню администратора. Все действия, выполняемые администратором при настройке и эксплуатации системы *Электронный замок*, осуществляются из этого меню.

Выберите пункт **настройка общих параметров** и нажмите клавишу *<Enter>*. На экране появится диалог управления системой *Электронный замок*, со следующими параметрами:

Параметр **“Минимальная длина пароля пользователя”** определяет минимальную длину пароля пользователя в символах. Пользователю нельзя назначить пароль, число символов в котором меньше числа, заданного этим параметром.

Параметр **“Предельное число неудачных входов пользователя”** определяет, сколько раз пользователь может допустить ошибку при входе в систему, указав неверный пароль. Если число неудачных входов пользователя в систему превысило число, заданное этим параметром, вход пользователя в систему будет блокирован.

Параметр **“Плата функционирует в автономном режиме”** определяет режим доступа любых внешних программ к области ОЗУ платы *Электронный замок*, в которой хранятся регистрационные записи системного журнала. В автономном режиме функционирования (значение параметра ‘Да’) любым внешним программам запрещается чтение информации из области памяти, хранящей записи системного журнала. Если этот режим выключен (значение параметра ‘Нет’) - внешним программам разрешен доступ на чтение к данной области ОЗУ платы *Электронный замок*. Этот режим может быть использован в том случае, если система защиты установлена на сетевой рабочей станции и необходимо интегрировать информацию системного журнала с нескольких рабочих станций (например, в случае использования системы *Электронный замок* совместно с системой защиты *Secret Net*).

Параметр **“Показ статистики пользователю”** позволяет разрешить или запретить вывод на экран при входе пользователя в систему информационного окна, содержащего сведения о его работе.

Параметр **“Тестировать ДСЧ для пользователя”** позволяет включить или отключить тестирование правильности работы датчика случайных чисел (ДСЧ) платы *Электронный замок*, осуществляющееся при входе пользователей в систему.

Параметр **“Контролировать целостность файлов”** позволяет включить или выключить контроль целостности объектов, осуществляющийся при загрузке пользователем операционной системы.

Чтобы приступить к управлению пользователями, выберите в меню администратора системы пункт **“Работа со списком пользователей”** и нажмите клавишу *<Enter>* /15/. На экране появится список пользователей (список имен пользователей), зарегистрированных в системе *Электронный замок*. В верхней части экрана располагается информационное окно, содержащее сведения о пользователе, имя которого выбрано в списке (после инициализации системы – список пользователей пуст). Для управления списком пользователей используйте клавиши, приведенные в строке сообщений.

Для регистрации нового пользователя:

- а) в режиме управления пользователями нажмите клавишу *<Insert>*;
- б) введите имя регистрируемого пользователя;
- в) на вопрос «Производится первичная регистрация пользователя?» ответьте «Да»;
- г) на запрос пароля пользователя введите пароль и его подтверждение, соблюдая указанные ранее требования к паролю;
- д) на запрос персонального идентификатора плотно прислоните к считывателю персональный идентификатор, присваиваемый пользователю, после этого появляется сообщение об успешном окончании регистрации.

Чтобы удалить пользователя из списка пользователей, зарегистрированных в системе *Электронный замок*:

- а) в режиме управления пользователями выберите имя удаляемого пользователя и нажмите клавишу *<Delete>*;
- б) для подтверждения удаления пользователя, нажмите клавишу *<Enter>*.

Чтобы изменить пароль пользователя

- а) в режиме управления пользователями выберите имя пользователя и нажмите клавишу *<Tab>*;
- б) на запрос персонального идентификатора прислоните к считывателю персональный идентификатор;

Далее процедура смены пароля пользователя соответствует процедуре ввода пароля администратора.

Чтобы изменить информацию о пользователе

- а) в режиме управления пользователями выберите имя пользователя и нажмите клавишу *<Enter>*;
- б) в появившемся экране с помощью клавиш управления, приведенных в строке сообщений вы можете изменить следующую информацию о пользователе:
 - сбросить (приравнять нулю) число неудачных попыток входа пользователя в систему);
 - изменить статус пользователя;
 - разрешить или запретить пользователю загрузку операционной системы с гибкого диска и CD ROM диска;
 - установить для пользователя режим работы подсистемы контроля целостности.
- в) после внесения изменений в информацию о пользователе подтвердите их в запросе сохранения изменений.

Для **настройки параметров работы подсистемы контроля целостности** выполните следующие действия:

- установите на компьютер программу формирования шаблонов контроля целостности в варианте, соответствующем операционной системе, под управлением которой работает данный компьютер;
- сформируйте шаблоны заданий на контроль целостности;
- произведите расчет эталонных значений контрольных сумм для проверяемых объектов.

Шаблоны заданий на контроль целостности (шаблоны контроля целостности) содержат информацию о местоположении контролируемых файлов на жестком диске (полный путь к ним) и координаты контролируемых секторов жесткого диска.

Для формирования шаблонов в среде операционных систем Windows 9'х и Windows NT выполните:

- а) в меню [Программы] главного меню *Windows* выберите подменю [Соболь], а в этом подменю выберите пункт [Программа подготовки шаблонов];
- б) после выполнения проверки существующих шаблонов контроля целостности и построения дерева файловой структуры жесткого диска (дисков) компьютера выберите необходимую закладку, содержащую название объекта (Файлы или Сектора);
- г) с помощью стандартных операций над деревом объектов отметьте символом $\sqrt{\quad}$ необходимые файлы (сектора);
- д) для сохранения шаблона нажмите кнопку [Сохранить].

После формирования шаблонов заданий на контроль целостности, выполните расчет эталонных значений контрольных сумм для объектов (файлов и секторов), заданных сформированными шаблонами:

- а) перезагрузите компьютер и войдите в систему с правами администратора;
- б) выберите в меню администратора системы пункт **“Расчет контрольных сумм”** и нажмите клавишу *<Enter>*.

Расчет контрольных сумм считается завершившимся успешно, если в процессе расчета не зафиксировано ни одной ошибки (поле “Найдено ошибок:” содержит значение “0”). В этом

случае осуществляется возврата к меню администратора. При возникновении ошибок откорректируйте шаблоны заданий на контроль целостности, исключив из них файлы, отсутствующие на диске, и заново произведите расчет эталонных значений контрольных сумм.

Просмотр записей системного журнала. Для просмотра записей системного журнала выберите в меню администратора пункт **“Работа с журналом регистрации событий”** и нажмите клавишу *<Enter>*. Окно *“Журнал регистрации событий”* содержит список записей, представленный в виде таблицы. Записи приводятся в порядке убывания времени регистрации соответствующих им событий. Просмотр записей осуществляется клавишами ‘↑’ и ‘↓’.

При необходимости все записи системного журнала могут быть удалены (очистка системного журнала). Для этого нажмите клавишу ** и подтвердите удаление в появившемся запросе.

Для выхода из режима просмотра системного журнала и возврата к меню администратора нажмите клавишу *<Esc>*.

ЛЗ-11. Средства защиты несанкционированного копирования информации

Цель: Изучить и опробовать средства защиты от несанкционированного копирования информации. Студенты уясняют и выполняют задания ЛЗ и выполняют все работы по ним

Учебные вопросы:

11.1. Привязка программ к гибким и жестким магнитным дискам. Программные методы защиты от НСК: идентификация аппаратной и программной сред, идентификация исполняемого модуля

11.2. Средства анализа и копирования защищенных дисков и взламывания защиты программ

Литература:

1. Герасименко В. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат, 1994.
2. Шураков В. Обеспечение сохранности информации в системах обработки данных. - М.: Финансы и статистика, 1985.
3. Стенг Д., Мун С. Секреты безопасности сетей. - Киев: Диалектика, 1996.

11.1. Привязка программ к гибким и жестким магнитным дискам. Программные методы защиты от НСК: идентификация аппаратной и программной сред, идентификация исполняемого модуля

Для примера работы средств защиты программ от копирования и преодоления такой защиты рассмотрим работу программ «НОТА» и INTRUDER /17/.

Программный комплекс «НОТА» позволяет выполнять привязку программ к ключевым меткам, расположенным на гибком или жестком магнитных дисках.

НОТА использует для привязки программ информацию, записанную в инженерные цилиндры.

Задание 1:

Войти в систему под именем user01 (рабочее место –01).

Скопируйте в свой рабочий каталог программу test.exe, запустите ее.

Запустите программу «НОТА» - Not.a.exe .

Просмотрите всю информацию, выполнив крайнюю левую команду меню.

Выполните команду Параметры и заполните соответствующие окна:

имя защищаемого файла;

имя защищенного файла (оба имени - полные);

копирование - диск, на котором будет проставлена метка для привязки программы (C:);

предельная дата использования программы (не заполнять);

допустимое число запуска программы (не заполнять);

уровень сложности защиты (не заполнять).

Выполните команду Защита. Запустите защищенную программу. Скопируйте защищенную программу в какой-нибудь каталог и попробуйте запустить.

Выполните защиту программы test.exe а) с привязкой к диску C и установкой предельной даты запуска – a.exe, в) с установкой уровня защиты 04 – b.exe, с) с привязкой к диску A и установкой числа запусков (3) – c.exe.

Проверить эффективность защиты от НСК, результаты испытаний протоколировать.

Сделать выводы о работоспособности СЗИ НОТА и эффективности защиты программ от НСК.

11.2. Средства анализа и копирования защищенных дисков и взламывания защиты программ

Одной из программ, разработанных взломщиками для вскрытия защиты программ, является программа INTRUDER.

INTRUDER предназначен для снятия внешней защиты программ, скомпилированных на TurboPascal/Borland Pascal 7.0, Microsoft C, Borland C++, Turbo C. При этом смысл внешней защиты несущественен - это может быть и упаковщик, и привязка к дискете/компьютеру и т.д. - INTRUDER все равно приводит программу к тому виду, в котором она была после компиляции (или стремится максимально приблизиться к этому).

INTRUDER во многих случаях определяет размер кода с точностью ДО БАЙТА. В тех случаях, когда не удастся точно определить размер кода, INTRUDER стремится максимально приблизить его размер к истинному. В случае точного определения конца кода результирующий размер будет отличаться от исходного на 32 байта для программ, написанных на BP/TP, максимум на 40-50 байт для BCPP/TC программ и, наконец, для MSC длина кода не отличается от истинной.

INTRUDER можно использовать с любыми программами. Если startup-код найден - вы тут же получите крэкованный исполняемый файл, если нет - ваша программа просто запустится и все. Для открэковки запустите INTRUDER [имя_файла_для_открэковки] [ключи_для_файла_для_открэковки]. Если все прошло нормально - получаете CRACKED.EXE. В качестве параметра можно указывать не только .EXE, но и .COM файлы (типа WD.COM), и даже .BAT - запуск производится через командный процессор, указанный в переменной COMSPEC.

Задание 2:

Запустите программу INTRUDER, указав в качестве параметра имя копии защищенного файла. Вы получите файл с именем CRACKED.EXE. Запустите этот файл на выполнение. При необходимости файлу можно присвоить прежнее имя.

Несмотря на установленную защиту, файл восстанавливается и получает способность выполняться с любого диска.

Выполните защиту программы test1.com с привязкой к диску C. Проверить эффективность защиты от НСК, выполнить взлом защиты, запустив программу INTRUDER, результаты испытаний протоколировать. Сделать выводы о работоспособности СЗИ НОТА и эффективности защиты программ от НСК.

В качестве примера программы, предназначенной для преодоления защиты дискет от копирования рассмотрим программу производства компании МЕДИНКОМ (Россия) Floppy Disk Analyser версии 6.1 /18/.

Задание 3:

Запустите программу FDA.EXE из каталога D:\FDA.

После запуска FDA на экране появляется основное меню из 11 пунктов, нажмите F1 для получения справки по каждому пункту меню. Выполнив калибровку, выйдите в основное меню и выполните пункт "Save Settings" (выполняется один раз после установки FDA).

Вставьте в дисковод дискету, которую необходимо скопировать.

Выполните команду Analyse & Read Disk (Анализ и чтение диска). (На 3.5" дискетах 82 цилиндра).

Для просмотра содержания формата считанной дискеты выполните команду View Disk Report File.

Для просмотра содержания дискеты выполните команду View Disk Data File.

Создание копий дискет на основе полученной при анализе информации проводится командой Format & Write Disk.

Выполните эту команду, вставив в дисковод чистую дискету.

Протоколы всех испытаний и выводы представить руководителю.

ЛЗ-12. Исследование программ, защищенных от копирования

Цель: Изучить и опробовать технологию исследования программ, защищенных от копирования. Студенты уясняют и выполняют задания ЛЗ и выполняют все работы по ним

Учебные вопросы:

- 12.1. Исследование программ с защитой от копирования
- 12.2. Исследование дискет, защищенных от копирования

Литература:

1. Герасименко В. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат, 1994.
2. Шураков В. Обеспечение сохранности информации в системах обработки данных. - М.: Финансы и статистика, 1985.
3. Стенг Д., Мун С. Секреты безопасности сетей. - Киев: Диалектика, 1996.

12.1. Исследование программ с защитой от копирования

Исследование программ с защитой от копирования будет проводиться с помощью

- дизассемблера Hiew,
- отладчика AFD и
- отладчика TD.

Hiew (Hacker's view) - это 'гляделка' для тех, кому требуется иногда в чужой программе изменить один-два байта (как правило, 7xh на 0EBh). Hiew позволяет просматривать файлы неограниченной длины в текстовом и шестнадцатеричном форматах, а также в режиме дизассемблера процессора Pentium(R) Pro. Переключение режимов – клавишей Enter.

Возможности:

1. Редактирование в шестнадцатеричном режиме и в режиме дизассемблера - клавишей F3
2. Встроенный ассемблер Pentium(R) Pro - клавишей F2, сохранение – F9.
3. Help контекстно-зависимый, откликается на F1.
4. Переходы по call/jmp в дизассемблере по цифрам '1'-'9'. Поиск ссылки на текущую позицию – F6. Определение заголовка EXE-программы – F8, переход на точку входа – F5.
5. Базирование - для тех, кому надо, чтобы .com обязательно начинался с 100h, и кто хочет, чтобы смещение в сегменте данных начиналось с нуля. База - это просто константа, которая прибавляется к смещению и адресам перехода, задается через Ctrl-F5.
6. Поиск ассемблерных команд по шаблону (для истинного хакера!)

В режиме дизассемблера можно искать команды по шаблону. В качестве (*) используется "?". То есть если при вводе ассемблерной команды встречается в строке символ "?" то пойдет поиск по шаблону, если нет - команда просто ассемблируется.

Например: в режиме DECODE <F7><F7> "mov ax,?" будет искать "mov ax, 1234h", "mov ax,sp", и т.д.

Можно искать последовательность команд, разделяя их точкой с запятой.

Например: "push ?10; call ?; add ?"

найдет связку:

не найдет:

```
-----
push 00010
call 01234:05678
add sp,00006
```

```
-----
push 00010
push 00011
add ax,00006
```

7. Для за/расшифровки кода/данных по сравнительно простому алгоритму - клавиши F3/F8. За один раз за/расшифровывается один байт/слово.

Задание 1:

1. Выполнить программу test1.com из каталога FDA. Провести анализ с помощью дизассемблера Hiew, затем выполнить в пошаговом режиме в отладчике AFD (клавишей F1) и отладчике TD (клавишей F7).

2. Выполнить защиту программы test1.com с помощью программы НОТА, получить файл testz.exe, привязанный к ключевой дискете.

3. Выполнить в пошаговом режиме в отладчике AFD (клавишей F1), затем провести анализ с помощью дизассемблера Hiew: найти область кода, область данных, точку входа.

4. Выполнить атаку на защищенную программу. Определить адрес начала исходной программы -adrnnn, заменить первую команду в точке входа на команду JMP adrnnn. Скорректировать адрес начала текстовой строки, загружаемый в регистр dx в команде mov dx,adr. Адрес должен быть на 200h меньше, чем реально видимый на экране (объяснить это явление).

5. Проверить эффективность защиты от НСК, результаты испытаний протоколировать. Запустить взломанную программу, проверить отсутствие защиты.

6. Сделать выводы об эффективности защиты программ от НСК СЗИ НОТА, о методе реализации защиты, методах взлома защиты программ.

Протоколы испытаний и выводы представить руководителю.

12.2. Исследование дискет, защищенных от копирования

Исследование дискет, защищенных от копирования, будет проводиться с помощью анализатора дискет FDA /18/.

Профессиональный анализатор дискет FDA позволяет не только точно копировать защищенные дискеты, но также подробно анализировать и исследовать формат и данные всех дорожек и секторов дискеты, при необходимости произвольно модифицировать их. Имеется возможность самостоятельного конструирования нестандартных форматов и ключевых меток любой сложности, быстрого тиражирования защищенных дискет. Работа с профессиональным вариантом требует некоторой подготовки пользователя, т.е. он должен знать строение дорожек, секторов и т.д. Достаточная для этого техническая информация имеется в прилагаемой документации.

Задание 2:

1. Выполните защиту программы test.exe с привязкой к диску А и установкой числа запусков (3) с именем tz.exe.

2. Запустите программу FDA.EXE из каталога D:\FDA.

После запуска FDA на экране появляется основное меню из 11 пунктов, для получения справки по каждому пункту меню нажмите F1.

3. Вставьте в дисковод дискету, которую необходимо анализировать.

4. Выполните команду Analyse & Read Disk (Анализ и чтение диска). (На 3.5" дискетах 82 цилиндра)

5. Выполните команду Open Operating Directory (Получение доступа к рабочим файлам) - ввести полный путь к операционным файлам (т. е. каталогу, содержащему файлы DISK.FMT, DISK.WRI и DISK.BIN), затем для просмотра содержания формата дискеты выполните команду View Disk Report File.

6. Выполните команду - Track Operations (Операции с отдельно выбранной дорожкой) - Переход в другое текстовое меню для выбора операций с одной отдельно выбранной дорожкой (№ 80 и 81): выполните анализ и чтение отдельной дорожки; просмотр Report файла дорожки; просмотр данных дорожки.

7. Сделать выводы об уязвимости реализации средства защиты от НСК с использованием ключевых дискет. Протоколы испытаний и выводы занести в отчет и представить руководителю

ЛЗ-13. Защита программ от изучения

Цель: Изучить и опробовать технологию защиты программ от изучения. Студенты уясняют и выполняют задания ЛЗ, а затем выполняют все работы по ним

Учебные вопросы:

13.1. Защита программ от дизассемблирования

Литература

1. Расторгуев С. Программные методы защиты информации в компьютерах и сетях. - М.: Яхтсмен, 1993.
2. Спесивцев А. и др. Защита информации в ПЭВМ. - М.: Радио и связь, 1993.

Для затруднения дизассемблирования подходит шифрование отдельных участков программ или всей программы целиком.

Способ динамического преобразования заключается в следующем: первоначально в оперативную память загружается фрагмент кода, содержание части команд которого, не соответствует тем командам, которые данный фрагмент в действительности выполняет; затем этот фрагмент по некоторому закону преобразуется, превращаясь в исполняемые команды, которые затем и выполняются.

Рассмотрим пример простейшего расшифровщика полиморфного вируса, созданного на основе общей схемы, предложенной в [2]:

00000100: 33DB	xor	bx,bx	
00000102: BE1101	mov	si,00111 ;"___"	
00000105: 8A00	mov	al,[bx][si]	
00000107: 3401	xor	al,001 ;"_"	
00000109: 8800	mov	[bx][si],al	
0000010B: 43	inc	bx	
0000010C: 83FB60	cmp	bx,060 ;"^^"	
0000010F: 75F4	jne	000000105 ----- (1)	
00000111: 8DC9	lea	cx,cx	
00000113: 8FD9	pop	cx	

Как будет показано далее, строки 105-109 реализуют механизм наложения маски на код программы.

Алгоритм работы этой части программы состоит в следующем.

1. Поместить в регистр al содержимое ячейки, расположенной по адресу ds:[si+bx].
2. Произвести побитовое сложение по модулю 2 содержимого регистра al и числа 01.
3. Записать обратно в ячейку ds:[si+bx] результат, полученный на предыдущем шаге.

Согласно листингу значение регистра bx полагается равным 0000, а это означает, что инструкции программы, расположенные по адресам 105-109, осуществляют преобразование содержимого ячейки 111. Если обратить внимание на команды, расположенные по адресам 10B-10f, то становится очевидной организация циклического наложения маски на код, начинающийся с адреса 111.

Задание 1:

1. Запустите программу t1-10-3 из каталога ПЗ10-3.
2. Запустите Niew, загрузите в него ту же программу, определите область кода, область данных, проведите статический анализ кода.
3. Запустите отладчик TD, загрузите в него ту же программу. Выполните программу в пошаговом режиме.
4. Сделать выводы о работоспособности и эффективности защиты программ от дизассемблирования.

Протоколы испытаний и выводы представить руководителю.

13.2. Защита программ от отладки и трассировки по прерываниям

Способы защиты от отладки можно разделить на четыре класса.

1. Влияние на работу отладочного средства через общие программные или аппаратные ресурсы. В данном случае наиболее известны:

а) использование аппаратных особенностей микропроцессора (особенности работы очереди выборки команд, особенности реализации команд и т.д.

б) использование общего программного ресурса (например, общего стека) с отладочным средством и разрушение данных или кода отладчика, принадлежащих общему ресурсу, либо проверка использования общего ресурса только защищаемой программой (например, определение стека в области, критичной для выполнения защищаемой программы); Например:

```
xor ax,ax
mov es,ax
mov [save_ss],ss
mov [save_sp],sp
mov ss,ax          ; здесь происходит срыв стека
mov sp,0ah
mov ss,[save_ss]
mov sp,[save_sp]
```

в) переадресация обработчиков отладочных событий (прерываний) от отладочного средства к защищаемой программе. К этой группе средств относится: блокировка специальных "отладочных" прерываний процессора;

- блокировка прерываний от клавиатуры;
- замер времени выполнения контрольных участков программы;
- использование прерывания таймера.

2. Влияние на работу отладочного средства путем использования особенностей его аппаратной или программной среды.

3. Влияние на работу отладчика через органы управления или/и устройства отображения информации.

4. Использование особенностей работы управляемого человеком отладчика - навязывании для анализа избыточно большого объема кода.

Задание 2:

1. Запустите программу t2-10-3. Запустите отладчик TD, загрузите в него ту же программу. Выполните программу в пошаговом режиме.

2. Сделать выводы о работоспособности и эффективности защиты программ от отладки и трассировки по прерываниям.

3. Проведите статический и динамический анализ программы t3-10-3 (динамический анализ программы необходимо проводить на процессоре I486).

Протоколы испытаний и выводы представить руководителю.

Практическое занятие №15

Лз 15. Устройство и принципы функционирования СЗИ от НСД, работа в среде СЗИ

Цель: Изучить устройства и принципы функционирования СЗИ от несанкционированного доступа, а также принципы их работы в среде СЗИ. Студенты уясняют и выполняют задания ЛЗ и выполняют все работы по ним

15.1. Устройство и принципы функционирования систем защиты информации от НСД, работа администратора системы защиты ПЭВМ

15.2. Управление пользователями

Литература:

1. Герасименко В. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат, 1994.
2. Шураков В. Обеспечение сохранности информации в системах обработки данных. - М.: Финансы и статистика, 1985.
3. Стенг Д., Мун С. Секреты безопасности сетей. - Киев: Диалектика, 1996.

15.1. Устройство и принципы функционирования систем защиты информации от НСД, работа администратора системы защиты ПЭВМ

Система Secret Net может быть установлена только на компьютеры, оснащенные процессорами семейства INTEL X86 или совместимыми с ними, имеющие жесткий диск и работающие под управлением ОС Windows'9x (Windows 95, Windows 98) с файловой системой FAT16 или FAT32 /19, 20, 21/.

Объем свободного дискового пространства, необходимый для установки системы защиты, составляет 15 Мбайт. Минимальный объем оперативной памяти - 16 Мб.

Требования к конфигурации компьютера:

Элемент	Минимально	Рекомендуется
Процессор	486 DX 40 МГц	Pentium 100 МГц
Оперативная память	16 Мб	32 Мб
Жесткий диск (свободное пространство)	15 Мб	25 Мб
Видеоадаптер	VGA	VGA/SVGA
Монитор	цветной или монохромный	

Перед установкой системы Secret Net обязательно проверьте жесткие диски компьютера на наличие потерянных фрагментов при помощи программы SCANDISKW.EXE из поставки ОС Windows'9x и устраните выявленные дефекты. Затем проверьте компьютер на отсутствие вирусов.

Процедура установки системы Secret Net включает следующие операции:

1. запуск программы установки;
2. принятие лицензионного соглашения;
3. определение пароля администратора безопасности;
4. предварительная настройка системы защиты;
5. копирование файлов на жесткий диск и настройка компьютера;
6. присвоение атрибутов Secret Net локальным ресурсам файловой системы компьютера; завершение процедуры установки и перезагрузка компьютера.

Перед отработкой практических заданий необходимо изучить разделы 1,3 документа “Система защиты информации “Secret Net” версия 4.0 (автономный вариант); Руководство по администрированию” (файл Secret Net - Admin Guide.doc).

Задание 1: Установка Secret Net

1. Запустить программу установки Secret Net – setup.exe.

2. Установить пароль для пользователя SUPERVISOR – supervisor.
 3. В окне конфигурирования рабочей станции выбрать “Установка атрибутов по умолчанию”.

4. В окне завершения установки выбрать “Перезагрузить компьютер”.

В результате установки системы *Secret Net* в состав меню “Программы” будет добавлено подменю “Secret Net for Windows 9x”.

В это подменю будут включены следующие пункты:

- “Изменение пароля”,
- “Настройки системы”
- “Удаление Secret Net” и
- “Управление атрибутами”.

После установки системы Secret Net администратором системы защиты является пользователь с именем SUPERVISOR.

Настройка системы защиты и управление объектами Secret Net

Основной объем работ по настройке системы *Secret Net*, как правило, выполняется на этапе ввода системы защиты в эксплуатацию. После этого, при эксплуатации системы защиты, может потребоваться изменить некоторые параметры работы системы.

Настройка системы *Secret Net* состоит в настройке защитных механизмов. В процессе настройки осуществляются следующие действия:

1. настройка параметров и режимов работы системы защиты;
2. формирование списка пользователей компьютера и настройка их свойств;
3. формирование списка групп пользователей компьютера и включение пользователей в соответствующие группы;
4. установка атрибутов владения и атрибутов управления доступом на локальные ресурсы (диски, каталоги и файлы) файловой системы компьютера;
5. присвоение категорий конфиденциальности соответствующим локальным дискам компьютера и каталогам, находящимся на локальных дисках компьютера.

Над объектами системы *Secret Net* могут осуществляться следующие базовые операции управления:

1. объект может быть создан (операция создания объекта);
2. объект может быть переименован (операция назначения объекту нового имени);
3. объект может быть удален (операция удаления объекта);
4. свойства объекта могут быть изменены (операции присвоения объекту свойства из постоянного списка свойств и отмены присвоения свойства объекту).

В системе *Secret Net* существуют следующие основные группы объектов управления:

“Пользователи” - эти объекты определяют состав реальных пользователей компьютера и свойства каждого из них;

“Группы пользователей” - эти объекты определяют состав групп пользователей компьютера и состав пользователей, входящих в каждую из групп;


ресурсы компьютера - для этих объектов устанавливаются определенные атрибуты доступа и владения, а также категории конфиденциальности, которые определяют права пользователей компьютера на доступ к ресурсу. Под ресурсами компьютера в данном случае понимаются локальные диски, каталоги и файлы, размещенные на локальных дисках.

Управление объектами системы защиты позволяет администратору безопасности управлять работой пользователей компьютера, создавая для каждого из них рабочую среду в соответствии с требованиями, существующими в организации.

Управление объектами системы *Secret Net* осуществляется при помощи программы *Проводник (Explorer)*, входящей в состав ОС Windows.

Задание 2:


Создать на диске С папку с именем Document, в ней папки Conf и Sconf.

Запустить программу *Проводник*. В левой части окна программы найдите папку  Secret Net '9x, подведите к ней курсор мыши и нажмите правую кнопку мыши. В появившемся


контекстном меню выберите пункт **“Свойства”**. В появившемся окне **“Настройки Secret Net”** выбрать вкладку **“Режимы”**. В группе **“Общие”** установить отметку в поле выключателей **“Полномочное управление доступом”**, **“Режим использования хранителя экрана Secret Net”**. Нажать кнопку **“Применить”**. В группе **“Полномочное управление доступом”** установить отметку в поле выключателей **“Контроль потоков данных”**, **“Контроль буфера обмена”**, **“Печать документов из WinWord”**. Нажать кнопку **“Применить”**. На вкладке **“Дополнительно”** отредактировать список конфиденциальных (C:\Document\Conf\) и строго конфиденциальных (C:\Document\Sconf\) каталогов. Нажать кнопку **“Применить”**.

В *Проводнике* отметить диск C и нажать правую кнопку мыши. В появившемся меню выбрать пункт *Secret Net* и установить категорию конфиденциальности **“Конфиденциально”**. Соответственно для ранее созданных папок установить уровень конфиденциальности. Создать в *Блокноте* текстовые файлы **“cdoc.txt”** – сохранить в папке C:\Document\Conf и **“sdoc.txt”** – сохранить в папке C:\Document\Sconf.

15.2. Управление пользователями

В системе *Secret Net* каждому реальному пользователю компьютера ставится в соответствие объект системы защиты - **“Пользователь”** (или  User). Далее, под управлением пользователем будем понимать управление этим объектом.

Задание 3:

Вызовите на экран окно программы *Проводник (Explorer)*. В левой части окна программы *Проводник* выберите с помощью мыши папку  **Пользователи**, при этом в правой части окна программы *Проводник* отобразится список всех пользователей, зарегистрированных в системе защиты. Установите курсор мыши в правой части окна программы *Проводник* так, чтобы он не попадал ни на один из содержащихся там объектов и нажмите правую кнопку мыши. В открывшемся контекстном меню выберите пункт **“Создать”**, затем подпункт **“Пользователя”**. Создать 5 пользователей с именами User1 – User5. Определить свойства каждого пользователя, для чего выбрать в списке ярлык с именем пользователя, свойства которого необходимо изменить, нажать правую кнопку мыши и активизировать в открывшемся меню пункт **“Свойства”**. Установить следующие параметры для:

User1:

Вкладка **“Общие”** -> **“Пользователь заблокирован”**.

User2:

Вкладка **“Общие”** -> **“Ограничения по времени работы”** -> **“Назначить...”** в появившемся окне установить текущую неделю, во всех днях недели установить время работы с 15.00 до 20.00.

User3:

Вкладка **“Общие”** -> **“Уровень допуска”** -> **Отсутствует**.

User4:

Вкладка **“Общие”** -> **“Уровень допуска”** -> **Конфиденциально**.

User5:

Вкладка **“Общие”** -> **“Уровень допуска”** -> **Строго конфиденциально**.

Для всех пользователей установить:

Вкладка **“Общие”** отметить выключатели **“Запрос пароля”** и **“Постоянный пароль”** (кроме User5) и определить пароли соответственно USER1 – USER5

Вкладка **“Режимы”** снять отметку в выключателе **“Мягкий режим контроля атрибутов”**. Вкладка **“Запреты”**, поставить отметку **“ограничения для пользователей Windows ‘9x”**, нажать кнопку **“Список”** и в появившемся окне отметить все выключатели в настройках системы.

Вкладка **“Регистрация”** установить максимальную регистрацию событий.

Войти в систему под именем Supervisor и запустить Проводник. Перейти в папку Secret Net и удалить пользователей User1 – User3 и закрыть Проводник.

ЛЗ-16. Работа в среде СЗИ от НСД "Secret Net"

Цель: Изучить и опробовать работу в среде СЗИ от несанкционированного доступа "Secret Net".
Студенты уясняют и выполняют задания ЛЗ, а затем выполняют все работы по ним

Учебные вопросы:

16.1. Установка СЗИ "Secret Net".

16.2. Работа администратора системы защиты ПЭВМ при использовании СЗИ от НСД "Secret Net"

16.3. Работа пользователей ПЭВМ в защищенной среде.

Литература:

1. СЗИ "Secret Net" версия 4.0 (автономный вариант) Описание применения.
2. СЗИ "Secret Net" версия 4.0 (автономный вариант) Руководство по администрированию.
3. ССИ "Secret Net" версия 4.0 (автономный вариант) Руководство пользователя.

Общие положения

Система Secret Net может быть установлена только на компьютеры, оснащенные процессорами семейства INTEL X86 или совместимыми с ними, имеющие жесткий диск и работающие под управлением ОС Windows'9x (Windows 95, Windows 98) с файловой системой FAT16 или FAT32.

Объем свободного дискового пространства, необходимый для установки системы защиты, составляет 15 Мбайт. Минимальный объем оперативной памяти - 16 Мб.

Требования к конфигурации компьютера:

Элемент	Минимально	Рекомендуется
Процессор	486 DX 40 МГц	Pentium 100 МГц
Оперативная память	16 Мб	32 Мб
Жесткий диск (свободное пространство)	15 Мб	25 Мб
Видеоадаптер	VGA	VGA/SVGA
Монитор	Цветной или монохромный	

Перед установкой системы Secret Net обязательно проверьте жесткие диски компьютера на наличие потерянных фрагментов при помощи программы SCANDISKW.EXE из поставки ОС Windows'9x и устраните выявленные дефекты. Затем проверьте компьютер на отсутствие вирусов.

Процедура установки системы Secret Net включает следующие операции:

1. Запуск программы установки;
2. Принятие лицензионного соглашения;
3. Определение пароля администратора безопасности;
4. Предварительная настройка системы защиты;
5. Копирование файлов на жесткий диск и настройка компьютера;
6. Присвоение атрибутов Secret Net локальным ресурсам файловой системы компьютера;
7. Завершение процедуры установки и перезагрузка компьютера.

16.1. Установка СЗИ "Secret Net".

Запустить программу установки Secret Net – setup.exe.

Установить пароль для пользователя SUPERVISOR – supervisor.

В окне конфигурирования рабочей станции выбрать “Установка атрибутов по умолчанию”

В окне завершения установки выбрать “Перезагрузить компьютер”

В результате установки системы *Secret Net* в состав меню “Программы” будет добавлено подменю “Secret Net for Windows 9x”. В это подменю будут включены следующие пункты:

- **Изменение пароля;**
- **Настройки системы;**
- **Удаление Secret Net и**
- **Управление атрибутами.**

Действия пользователя при работе с компьютером, на котором установлена система защиты информации (СЗИ) *Secret Net*, подробно описаны в документе [3] (Система защиты информации “Secret Net” версия 4.0 (автономный вариант) Руководство пользователя).

После установки СЗИ *Secret Net* администратором системы защиты является пользователь с именем SUPERVISOR.

15.2. Работа администратора СЗ ПЭВМ при использовании СЗИ от НСД "Secret Net"

Настройка системы защиты и управление объектами Secret Net. Основной объем работ по настройке системы *Secret Net*, как правило, выполняется на этапе ввода системы защиты в эксплуатацию. После этого, при эксплуатации системы защиты, может потребоваться изменить некоторые параметры работы системы.

Настройка системы *Secret Net* состоит в настройке защитных механизмов. В процессе настройки осуществляются следующие действия:

1. Настройка параметров и режимов работы системы защиты;
2. Формирование списка пользователей компьютера и настройка их свойств;
3. Формирование списка групп пользователей компьютера и включение пользователей в соответствующие группы;
4. Установка атрибутов владения и атрибутов управления доступом на локальные ресурсы (диски, каталоги и файлы) файловой системы компьютера;
5. Присвоение категорий конфиденциальности соответствующим локальным дискам компьютера и каталогам, находящимся на локальных дисках компьютера.

Над объектами системы *Secret Net* могут осуществляться следующие базовые операции управления:

1. объект может быть создан (операция создания объекта).
2. объект может быть переименован (операция назначения объекту нового имени).
3. объект может быть удален (операция удаления объекта).
4. свойства объекта могут быть изменены (операции присвоения объекту свойства из постоянного списка свойств и отмены присвоения свойства объекту).

В системе *Secret Net* существуют следующие основные группы объектов управления:

- **Пользователи** - эти объекты определяют состав реальных пользователей компьютера и свойства каждого из них;


- **Группы пользователей** - эти объекты определяют состав групп пользователей компьютера и состав пользователей, входящих в каждую из групп;

- **Ресурсы компьютера** - для этих объектов устанавливаются определенные атрибуты доступа и владения, а также категории конфиденциальности, которые определяют права пользователей компьютера на доступ к ресурсу. Под ресурсами компьютера в данном случае понимаются локальные диски, каталоги и файлы, размещенные на локальных дисках.

Управление объектами СЗИ позволяет администратору безопасности управлять работой пользователей компьютера, создавая для каждого из них рабочую среду в соответствии с требованиями, существующими в организации.

Управление объектами системы *Secret Net* осуществляется при помощи программы *Проводник (Explorer)*, входящей в состав ОС *Windows*.


Создать на диске С папку с именем Document, в ней папки Conf и Sconf.


Запустить программу *Проводник*. В левой части окна программы найти папку  Secret Net '9x, подвести к ней курсор мыши и нажать правую кнопку мыши. В появившемся контекстном меню выбрать пункт “Свойства”. В появившемся окне “Настройки Secret Net”

выбрать вкладку “Режимы”. В группе “Общие” установить отметку в поле выключателей **“Полномочное управление доступом”**, **“Режим использования хранилища экрана Secret Net”**. Нажать кнопку “Применить”. В группе “Полномочное управление доступом” установить отметку в поле выключателей **“Контроль потоков данных”**, **“Контроль буфера обмена”**, **“Печать документов из WinWord”**. Нажать кнопку “Применить”. На вкладке “Дополнительно” отредактировать список конфиденциальных (C:\Document\Conf\) и строго конфиденциальных (C:\Document\Sconf\) каталогов. Нажать кнопку “Применить”.

В *Проводнике* отметить диск C и нажать правую кнопку мыши. В появившемся меню выбрать пункт *Secret Net* и установить категорию конфиденциальности “Конфиденциально”. Соответственно для ранее созданных папок установить уровень конфиденциальности. Создать в *Блокноте* текстовые файлы “cdoc.txt” – сохранить в папке C:\Document\Conf и “sdoc.txt” – сохранить в папке C:\Document\Sconf.

16.3. Работа пользователей ПЭВМ в защищенной среде.

Управление пользователями. В системе *Secret Net* каждому реальному пользователю компьютера ставится в соответствие объект системы защиты - **“Пользователь”** (или  User). Далее, под управлением пользователем будем понимать управление этим объектом.

Вызовите на экран окно программы *Проводник (Explorer)*. В левой части окна программы *Проводник* выберите с помощью мыши папку  Пользователи, при этом в правой части окна программы *Проводник* отобразится список всех пользователей, зарегистрированных в системе защиты. Установите курсор мыши в правой части окна программы *Проводник* так, чтобы он не попадал ни на один из содержащихся там объектов и нажмите правую кнопку мыши. В открывшемся контекстном меню выберите пункт **“Создать”**, затем подпункт **“Пользователя”**. Создать 5 пользователей с именами User1 – User5. Определить свойства каждого пользователя, для чего выбрать в списке ярлык с именем пользователя, свойства которого необходимо изменить, нажать правую кнопку мыши и активизировать в открывшемся меню пункт **“Свойства”**.

Установить следующие параметры для:

User1:

Вкладка “Общие” -> “Пользователь заблокирован”.

User2:

Вкладка “Общие” -> “Ограничения по времени работы” -> “Назначить...” в появившемся окне установить текущую неделю, во всех днях недели установить время работы с 15.00 до 20.00.

User3:

Вкладка “Общие” -> “Уровень допуска” -> Отсутствует.

User4:

Вкладка “Общие” -> “Уровень допуска” -> Конфиденциально.

User5:

Вкладка “Общие” -> “Уровень допуска” -> Строго конфиденциально.

Для всех пользователей установить:

Вкладка “Общие” отметить выключатели “Запрос пароля” и “Постоянный пароль” (кроме User5) и определить пароли соответственно USER1 – USER5

Вкладка “Режимы” снять отметку в выключателе “Мягкий режим контроля атрибутов”. Вкладка “Запреты”, поставить отметку “ограничения для пользователей Windows ‘9x” , нажать кнопку “Список” и в появившемся окне отметить все выключатели в настройках системы.

Вкладка “Регистрация” установить максимальную регистрацию событий.

Перезагрузить компьютер и войти по очереди под именами User1 – User5 и отредактировать созданные текстовые файлы. Закрывать все работающие программы и нажать клавиши Ctrl+F12. Работая под именем User5 выбрать “Пуск”-> “Программы”-> “Secret Net 4.0”-> “Изменение пароля” и изменить пароль. Перезагрузить компьютер и войти под именем User5 со старым паролем, повторить попытку ввода старого пароля 3 раза.

Войти в систему под именем Supervisor и запустить Проводник.

Перейти в папку Secret Net и удалить пользователей User1 – User3.

Закрыть Проводник.

Удалить СЗИ Secret Net, для чего выполнить

1. “Пуск”-> “Программы”-> “Secret Net 4.0”-> “Удаление Secret Net”.
2. В окне “Удаление Secret Net for Windows ’9x” выбрать “удаление Secret Net с рабочей станции”, “восстановить файлы...” и “перезагрузить рабочую станцию...”

ЛЗ-17. Защита информации в ЛВС NetWare

Цель: изучить особенности реализации защиты от НСД в локальной вычислительной сети (ЛВС) NetWare и практически ознакомиться с основными инструментами администратора и процедурами управления сетью.

Учебные вопросы:

- 17.1. Работа администратора ЛВС NetWare по управлению пользователями
- 17.2. Работа администратора ЛВС NetWare по управлению доступом пользователей и процессов к ресурсам системы
- 17.3. Утилиты ОС, применяемые для обеспечения защиты информации

Литература:

1. Герасименко В. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат, 1994.
2. Шураков В. Обеспечение сохранности информации в системах обработки данных. - М.: Финансы и статистика, 1985.
3. Стенг Д., Мун С. Секреты безопасности сетей. - Киев: Диалектика, 1996.
4. Расторгуев С. Программные методы защиты информации в компьютерах и сетях. - М.: Яхтсмен, 1993.
5. Спесивцев А. и др. Защита информации в ПЭВМ. - М.: Радио и связь, 1993.

Включение компьютера и регистрация в ЛВС

1. Включить персональный компьютер.
2. В загрузочном меню DOS выбрать команду «**Работа с NETWARE**».

До выполнения процедуры регистрации в сети пользователю на файл-сервере доступен каталог SYS:LOGIN с правами чтения и просмотра, отображаемый на локальный логический диск F:.

3. Выполнить регистрацию командой **LOGIN**.
4. Ввести имя пользователя: userX;
пароль пользователя: pswrdX,
где имя X - номер рабочей станции пользователя.

С этого момента пользователю становятся доступны сетевые ресурсы файл-сервера: каталоги LOGIN, PUBLIC с правами чтения и просмотра (R, F), MAIL (подкаталог с сетевым номером пользователя), USERX, где X – номер рабочей станции пользователя, со всеми правами.

5. Просмотреть свои права в этих каталогах командой **RIGHTS**.

17.1. Работа администратора ЛВС NetWare по управлению пользователями

1. Работа с утилитой SYSCON. Утилита SYSCON (SYSstem CONfiguration - системная конфигурация) - инструмент администратора сети. Как администратор Вы по своим полномочиям являетесь менеджерами своих одноименных групп и можете использовать эту утилиту для управления пользователями своей рабочей группы.

Запустить SYSCON.

Перед Вами главное меню утилиты.

Нажать клавишу F1 и просмотреть комментарий справки по всем доступным командам.

Выйти из справки.

Выделить команду меню **Информация о клиентах** и нажать клавишу Enter (в дальнейшем под выполнением команды меню понимается высвечивание этой команды и нажатие клавиши Enter).

В появившемся окне выбрать группу с *именем, совпадающим с вашим*, и нажать Enter. Это группа, менеджером которой Вы являетесь.

Просмотреть доступную информацию о группе, выбирая соответствующие опции в открывшемся окне. При необходимости нажать F1 и ознакомиться со справкой по содержанию этих опций.

Выйти в главное меню программы, нажав необходимое число раз клавишу Esc (в дальнейшем под процедурой выхода в старшее меню понимается нажатие соответствующее количество раз клавиши Esc).

Выполнить команду **Информация о клиентах**.

Просмотреть доступную информацию о клиентах системы, при необходимости просмотреть справку.

Выполнить команду **Назначение опекуна в каталог**. Просмотрите Ваши полномочия в доступных каталогах, нажав Enter на имени каталога.

Выйти в предыдущее окно.

2. Создание клиентов

Нажать клавишу Ins для создания нового пользователя.

Ввести имя нового клиента – **USERX_1**, где X – номер вашей рабочей станции, что будет подразумеваться и при дальнейшем подобном именовании.

В качестве домашнего каталога указать **SYS:USERX\USERX_1**.

Выполните команду **Ограничения бюджета**, ознакомьтесь со справкой по опциям, содержащимся в открывшемся окне.

Выполните команду **Ограничения времени**. Ознакомьтесь со справкой, попробуйте изменить назначенные установки. Например, удалите из доступного времени промежутки 0.00–7.30, 17.00–24.00.

Выполнением следующих операций Вы включите нового клиента в управляемую Вами группу.

Выполнить команду **Информация о группах**, выберите свою группу, затем откройте окно **Члены группы**. Нажмите клавишу Ins. В дальнейшем для добавления новых элементов в списки используется клавиша INS.

В открывшемся окне появился список пользователей, не являющихся членами группы. Выберите имя созданного Вами нового пользователя, и нажмите Enter.

Выйти из программы SYSCON нажатием клавиши Esc.

Зарегистрироваться в сети под именем нового клиента. Вместо пароля нажать клавишу Enter. Система предложит Вам сменить пароль. Введите новый пароль pswrdX_1.

Для изменения пароля самим пользователем служит утилита SETPASS.

Выполните команду SETPASS и введите какой-либо новый пароль.

Просмотрите права созданного Вами пользователя в доступных каталогах.

17.2. Работа администратора JIBC NetWare по управлению доступом пользователей и процессов к ресурсам системы.

1. Управление правами клиентов.

Зарегистрируйтесь под именем userX.

Запустите SYSCON.

Команды **Информация о клиентах**, **USERX_1**, **Назначение опекуна в каталоги**.

Нажмите клавишу Ins. Введите имя назначаемого каталога: **SYS:USERX**.

Просмотрите права пользователя USERX_1 в назначенном каталоге. Новые права можно назначить нажатием Ins и выбором из доступного набора прав.

Выйти из SYSCON.

Для назначения прав пользователям в режиме командной строки служит утилита GRANT.

Выполнить команду:

GRANT /?

Ознакомьтесь с синтаксисом команды.

Выполнить команду:

GRANT R C F FOR SYS:USER TO USERX_1

Зарегистрироваться как USERX_1, просмотреть свой права в доступных каталогах, сравнить с имевшимися ранее.

Зарегистрироваться как USERX.

Запустить SYSCON.

Выполнить команды: **Информация о клиентах, USERX_1, Назначение опекуна в каталог.**

Добавить к назначенным каталогам **SYS:USERX\USERX_1**. В качестве назначенных прав указать **ВСЕ ПРАВА**, перечисленные в списке. Для одновременного назначения некоторого подмножества списка элементов используется выделение клавишей F5.

Выйти из SYSCON.

2. Управление атрибутами файлов.

Скопировать из каталога PUBLIC в каталог USERX_1 несколько файлов. Перейти в этот каталог.

Для просмотра и изменения атрибутов файлов предназначена утилита FLAG.

Выполнить команду:

FLAG /?

Ознакомиться со списком возможных атрибутов (расшифровка – выше).

Выполнить команду **FLAG**. Просмотреть атрибуты файлов в каталоге.

Установите для одного из файлов атрибут Только выполнение (X):

FLAG имя_файла X

Попробуйте установить другие атрибуты.

Кроме утилит командной строки для управления атрибутами файлов предназначена интерактивная утилита FILER.

Запустить FILER из каталога PUBLIC.

Выбрать текущим каталог **SYS:USERX\USERX_1**.

Выполнить команду **Информация о каталоге**. Просмотреть справку по содержанию опций, перечисленных в открывшемся окне.

Выбрать опцию **Наследуемые права** – описание маски наследуемых прав: прав, наследуемых файлами от каталога. Добавление и удаление наследуемых прав осуществляется соответственно клавишами Ins, Del (как и во всех списках системы). Измените маску наследуемых прав.

Выйти в основное меню программы.

Выполнить команду **Содержимое каталога**.

Выделить какой-либо файл. Просмотреть информацию о файле. Изменить атрибуты доступа и содержание маски наследуемых прав.

Установите для какого-либо файла атрибут **Очистка** (Окончательное удаление без возможности восстановления).

Выйти из FILER.

Перейти в каталог USERX_1.

Просмотреть атрибуты файлов. Сравнить с предыдущими значениями.

17.3. Утилиты ОС, применяемые для обеспечения защиты информации.

1. Восстановление удаленных файлов.

Удалить несколько файлов из каталога USERX_1.

Если система сообщает, что какой-либо файл не может быть удален, измените его атрибуты командой:

FLAG имя_файла N

и снова попытайтесь его удалить.

Для восстановления ошибочно удаленных файлов предназначена утилита SALVAGE.

Запустите программу SALVAGE из каталога PUBLIC.

Ознакомьтесь со справкой по утилите.

Просмотрите файлы, которые можно восстановить, соответствующей командой системы.

Закройте SALVAGE.

Просмотрите результаты восстановления файлов.

2. Создание большого числа подобных клиентов. Одновременное внесение в систему большого количества клиентов с одинаковыми полномочиями по доступу к системе требует от администратора больших затрат труда. Для облегчения работы администраторов системы предназначены специальные утилиты MAKEUSER и USERDEF.

Познакомимся с утилитой USERDEF.

Запустить USERDEF.

Для создания клиентов программа использует специальные шаблоны с описанием основных параметров клиентов. В системе может быть несколько шаблонов. Шаблон по умолчанию – DEFAULT.

Для редактирования шаблонов и создания новых Вы должны обладать правами записи в каталог PUBLIC.

Выполнить команду **Просмотр и редактирование шаблонов**. Ознакомьтесь со справкой.

Для создания нового шаблона необходимо нажать клавишу Ins и затем ввести имя шаблона.

Попробуйте изменить содержание шаблона. Выход из окна редактирования – клавиша Esc. Система предложит Вам сохранить новый шаблон, но при попытке записи на диск операция будет прервана из-за отсутствия права записи в каталог.

Снова запустите программу и создайте клиента с использованием шаблона DEFAULT.

Выбрать шаблон, нажать Enter. Затем, по появлении списка клиентов нажать Ins.

Система предложит ввести полное имя и имя регистрации клиента. Введите USERX_2 в обоих случаях. По умолчанию полное имя клиента используется системой в качестве первоначального пароля.

Создайте еще несколько клиентов с подобными именами, изменяя номер.

Нажмите клавишу Esc.

После закрытия окна клиентов система предложит Вам создать описанных клиентов. Подтвердите свое желание.

В ходе создания клиентов программа сообщит об ошибках при создании домашних каталогов (из-за использования шаблона DEFAULT и отсутствия права записи в корневом каталоге тома SYS).

Зарегистрируйтесь под именами созданных Вами новых клиентов, по приглашению системы измените пароли, затем просмотрите свои права в доступных каталогах.

Зарегистрируйтесь как USERX.

Запустите SYSCON.

Удалите всех созданных Вами клиентов, выполнив команду **Информация о клиентах**, высвечивая имена клиентов и нажимая клавишу Del.

Выйдите из программы и удалите каталог USERX_1.

Закончите сеанс работы с ЛВС.

ЗАКЛЮЧЕНИЕ

В заключении дадим методологические советы бакалаврам, осваивающим практику применения теории информационной безопасности и защиты информации в своей будущей специальности.

Важная задача практического освоения технологий грамотного использования положений дисциплины "Информационная безопасность" в профессиональной деятельности выпускников КубГАУ по специальности 080500.62 – Бизнес информатика может быть успешно решена только в том случае, если на основе ее теоретических и прикладных положений студенты практически освоят работу по ее разделам

- организационно-правовой,
- инженерно-технической,
- аппаратно-программной и
- криптографической

Другими словами, научиться реализовать в своей деятельности указанные положения на уровне навыков, умений результативного применения всего арсенала средств и методов защиты информации в АИС, доведя их до высшей степени совершенства, т.е. до автоматизма. Но для этого надо без усталы работать с этими средствами и методами, совершенствовать свои умения и навыки их профессионального использования по специальности. Именно этому и способствует качественное выполнение каждым обучаемым всех сквозных практических заданий и подготовка ответов на контрольные вопросы практикума.

ЛИТЕРАТУРА

Основная:

1. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, 2006. – 264с.
2. Лаптев В.Н. Информационная безопасность и защита информации: Курс лекций. – Краснодар: КубГАУ, 2010. – 132с.
3. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический проект; Гаудеамус, 2007, - 544с.

Нормативная

4. Государственный стандарт Российской Федерации ГОСТ Р 50922-96. Защита информации. Основные термины и определения. Издание официальное Госстандарта России. – М.: Госстандарт РФ, 1996. – 34с.
5. Доктрина информационной безопасности РФ. – М.: Госстандарт РФ, 2003. – 42с.
6. Закон РФ "Об информации, информатизации и защите информации" № 24-ФЗ от 20 февраля 1995.
7. Информационная безопасность и защита информации: Справочник для студентов. /В.И. Лойко., В.Н. Лаптев, Д.Ю. Жмурко. – Краснодар: КубГАУ, 2010. - 100с.

Дополнительная:

9. Девянин П.Н. Теоретические основы компьютерной безопасности: Уч. пособие для вузов. /П.Н. Девянин, Д.И. Михальский, Д.И. Правиков, А.Ю.Щербаков – М.: Радио и связь, 2003. – 192с.
10. Жельников В. Криптография от папируса до компьютера. – М.: АБФ, 1997. - 241с.
11. Зегжда Д., Ивашко А. Как построить защищенную информационную систему. /Д. Зегжда, А. Ивашко.– СПб.: Мир и семья, 2003. – 98с.
12. Зима В. Компьютерные сети и защита передаваемой информации. /В. Зима, А. Молдовян., Н. Молдовян. – СПб.: СПбГУ, 2005. – 198с.
14. Мельников В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 2007. – 157с.
15. Расторгуев С. Программные методы защиты информации в компьютерах и сетях. - М.: Яхтсмен, 2004. – 154с.
16. Расторгуев С. Информационная война. - М.: Радио и связь, 1998. - 416с.
17. Трубачев А.П. и др. Оценка безопасности информационных технологий. - М.: Издательство СИП РИА, 2003. - 356с.

Лаптев Владимир Николаевич
Лаптев Сергей Владимирович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
Практикум для бакалавров специальности
080500.62 – Бизнес информатика

Лицензия ИД № 02334 от 14.07.2000

Подписано в печать
 Бумага офсетная
 Печ.л. 4,0
 Тираж экз.

Формат 60х84
 Офсетная печать
 Заказ №

Отпечатано в типографии КубГАУ, 350044, г. Краснодар, ул. Калинина, 13