

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

**Факультет прикладной информатики**  
*Кафедра компьютерных технологий и систем*

## **ЗАЩИТА ИНФОРМАЦИИ**

**Практикум для бакалавров**

**Краснодар**  
**КубГАУ**  
**2015**

**УДК 004**  
**ББК 32.81 я 7**  
**И72**

Рецензент:

• доктор технических наук, профессор Атрощенко В.А. – декан факультета компьютерных технологий и автоматизированных систем ФГОУ ВПО «Кубанский государственный технологический университет».

**И72 Защита информации: Практикум для бакалавров / В.Н. Лаптев, С.В. Лаптев, А.В. Параскевов. – Краснодар: ФГБОУ ВПО КубГАУ, 2015. – 84 с.**

Практикум по дисциплине «Защита информации» подготовлен в соответствии с требованиями Федерального государственного образовательного стандарта (ФГОС) высшего профессионального образования (ВПО) по направлению 230400.62 – «Информационные системы и технологии» для студентов факультета прикладной информатики ФГБОУ ВПО «Кубанский государственный аграрный университет».

Он является обязательным приложением к курсу лекций по дисциплине, так как обеспечивает проведение лабораторных занятий (ЛЗ) и выполнение самостоятельной работы студентами (СРС) по ней. Обеспечивает углубленное усвоение основ обеспечения защиты информации (ЗИ), качественное проектирование и эксплуатацию систем защиты информации (СЗИ) в АИС, грамотную работу с конфиденциальной информацией, аппаратно-программными и инженерно-техническими комплексами в защищенных компьютерных системах. Выполнение ЛЗ и подготовка ответов на экзаменационные вопросы по дисциплине способствуют эффективному применению знаний, умений и навыков по ЗИ на практике.

Практикум рассмотрен и рекомендован к изданию на заседании кафедры компьютерных технологий и систем КубГАУ 19 января 2015 г., протокол № 5.

**УДК 004**  
**ББК 32.81 я 7**

© Лаптев Владимир Николаевич,  
Лаптев Сергей Владимирович,  
Параскевов Александр Владимирович  
© ФГБОУ ВПО Кубанский государственный  
аграрный университет, 2015.

## Оглавление

<b>ВВЕДЕНИЕ.....</b>	<b>4</b>
<b>ЛАБОРАТОРНЫЕ ЗАНЯТИЯ .....</b>	<b>6</b>
ЛЗ-01. ИЗУЧЕНИЕ СИСТЕМЫ ОТЕЧЕСТВЕННЫХ СТАНДАРТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЕ ИНФОРМАЦИИ.....	6
ЛЗ-02. РАЗРАБОТКА МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ .....	8
ЛЗ-03. ПРОГРАММИРОВАНИЕ АРИФМЕТИЧЕСКИХ АЛГОРИТМОВ ШИФРОВАНИЯ .....	32
ЛЗ-04. ПРОГРАММИРОВАНИЕ АЛГЕБРАИЧЕСКИХ АЛГОРИТМОВ ШИФРОВАНИЯ .....	36
ЛЗ-05. КОНТРОЛЬ СОСТОЯНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ .....	39
ЛЗ-06. ИССЛЕДОВАНИЕ ПРОБЛЕМ ОЧИСТКИ МАГНИТНЫХ НОСИТЕЛЕЙ .....	49
ЛЗ-07. ПРИМЕНЕНИЕ ПРОГРАММНЫХ АНТИВИРУСНЫХ КОМПЛЕКСОВ .....	52
ЛЗ-08. АППАРАТНЫЕ СРЕДСТВА ОПОЗНАНИЯ ПОЛЬЗОВАТЕЛЕЙ.....	64
ЛЗ-09. СРЕДСТВА ЗАЩИТЫ НЕСАНКЦИОНИРОВАННОГО КОПИРОВАНИЯ ИНФОРМАЦИИ..	72
ЛЗ-10. ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ПАРОЛЯ .....	74
<b>ЗАКЛЮЧЕНИЕ.....</b>	<b>79</b>
<b>ЛИТЕРАТУРА .....</b>	<b>80</b>
<b>ПРИЛОЖЕНИЯ .....</b>	<b>81</b>
Приложение-1. ПРОГРАММА СРС по дисциплине.....	81
Приложение 2. Перечень УММ, по дисциплине .....	83
Приложение-3. Программное обеспечение, используемое на ЛЗ .....	84

## ВВЕДЕНИЕ

Практикум подготовлен с учетом опыта преподавания дисциплин по информационной безопасности и защите информации в высших учебных заведениях для технических и экономических специальностей в соответствии с требованиями их учебных планов, основных образовательных программ профессиональной подготовки (ООП) и Федеральных государственных образовательных стандартов (ФГОС) высшего профессионального образования (ВПО). Учтено, что требования ФГОС ВПО по направлению **230400.62 – Информационные системы и технологии** к освоению основных разделов дисциплины инженерами во многом идентичны аналогичным требованиям для бакалавров. Учитывая эту особенность, авторы попытались обобщить эти требования и предложить методику выполнения лабораторных занятий (ЛЗ) с учетом анализа мнений других ученых и преподавателей вузов, приведенных в списке литературы к данной работе.

Практикум является приложением к лекциям по **защите информации (ЗИ)**. Он предназначен для проведения лабораторных занятий (ЛЗ) и самостоятельной работы студентов (СРС) по ЗИ. В нем рассмотрены прикладные аспекты проектирования и использования систем защиты информации (СЗИ), приемы работы бакалавров с информацией, аппаратно-программными и инженерно-техническими комплексами в защищенных компьютерных системах. Выполнение предложенных ЛЗ и подготовка ответов на вопросы к экзамену по ЗИ призваны повысить качество обучения бакалавров.

Преподаватель, ведущий дисциплину "Защита информации", самостоятельно выбирает:

- тематику лекций;
- тематику ЛЗ;

Обучаемые имеют возможности выполнять все задания практикума самостоятельно или под руководством и контролем преподавателя. Поэтому, для полного освоения изучаемой дисциплины необходимо пользоваться указанной литературой и выполнить как можно больше заданий практикума. Работа позволяет получить общее представление о дисциплине «Защита информации».

### **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 обучающихся, 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 обучающийся от обучающихся: 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 методического и материального обеспечения занятия. Он лично заблаговременно готовит необходимые учебно-методические материалы (УММ) и проверяет, оборудование, которое должно использоваться при проведении ЛЗ. УММ должны обладать изобразительной наглядностью, быть поучительными, правильными и соответствовали содержанию учебных вопросов.

#### 2. Порядок оценки работы обучаемых на занятиях.

Работа на ЛЗ оценивается по следующим параметрам:

- за выполненное ЛЗ;
- за ответ на вопросы по их выполнению;
- за добавления;
- за конспект лекций.

По этим результатам выставляется суммарная оценка за ЛЗ.

#### 3. Критерии оценки.

Ответы обучаемых на учебные вопросы оценивается на «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Оценка «отлично» - выставляется, при методически грамотном изложении сути конкретного аспекта ЗИ, с помощью четких, логически завершенных формулировок, конкретных выводов.

Оценка «хорошо» – выставляется в случае правильного изложения сути ответа на учебный вопрос, но при наличии отдельных неточностей 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 обучаемый не знает ответа на учебный вопрос, сам заявляет преподавателю о незнании или не готовности к ответу на вопрос, не обладает логикой инженерного мышления, а также в тех случаях, когда не выполнены условия для выставления оценки "удовлетворительно".

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

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

## ЛАБОРАТОРНЫЕ ЗАНЯТИЯ

### **Лз-01. Изучение системы отечественных стандартов по информационной безопасности и защите информации** (2 часа)

**Цель занятия** – исследование и сравнение отечественных и зарубежных стандартов в области защиты информации и информационной безопасности. (ИБ).

Учебные вопросы:

1.1. Исследовать и сравнить отечественных и зарубежных стандартов в области защиты информации (ЗИ) и информационной безопасности. (ИБ).

1.2. Сравнить эти стандарты и оценить полезность их применения в РФ.

Литература:

1. Доктрина информационной безопасности РФ - сайт Правительства РФ, [www.gov.ru](http://www.gov.ru).
2. Харрис Н. CISSP. Руководство подготовки к экзамену. – М.: McGraw-Hill, 2012. – 1472с.
1. ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.
2. Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации.
3. ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.
4. ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
5. ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
6. ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
7. ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
8. ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий» — стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности — благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» — защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.
9. ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005.
10. ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005.
11. ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.

**Задание к работе**

1. Проанализировать содержание 11 стандартов в области защиты информации (ЗИ) и информационной безопасности (ИБ) в РФ.
2. Сравнить эти стандарты с аналогичной зарубежной нормативной базой в области ИБ и ЗИ. Оценить их применимость в России.

**Форма и содержание отчёта по занятию.**

Отчёт должен содержать:

1. Титульный лист.
2. Историю создания и развития стандартов и их связь со смежными документами.
3. Назначение и описание стандартов.
4. Практику применения стандартов в России.
5. Перечень использованных информационных источников.

## **ЛЗ-02. Разработка модели разграничения доступа к информации**

(4 часа)

**Цель занятия** – для конкретной объекта, использующего в своей деятельности автоматизированные системы (АС) и информационные технологии (ИТ), разработать перечень защищаемых ресурсов и определить их критичности. Установит категории персонала и программно-аппаратных средств, на которые распространяется политика информационной безопасности (ЗИ). Установить особенностей расположения, функционирования и построения средств компьютерной системы (КС) на объекте и выявить угрозы безопасности информации и класс его защищенности объекта. Сформировать требований к построению СЗИ на объекте и определить места уязвимости АС и выбрать средства защиты информации. Научить обучающихся разрабатывать модель системы защиты информации (СЗИ) для АС от несанкционированного доступа (НСД) на основе изучения влияния организационной и информационной структур систем управления (СУ) «своего» объекта на его информационную архитектуру и состав требований к защите информации.

Учебные вопросы:

- 2.1. Разработать перечень защищаемых ресурсов и их критичности.
- 2.2. Определить категории персонала и программно-аппаратных средств, на которые распространяется политика информационной безопасности.
- 2.3. Установить особенностей расположения, функционирования и построения средств компьютерной системы (КС) и выявить угрозы безопасности информации и класса защищенности АС.
- 2.4. Сформировать требований к построению СЗИ объекта автоматизации.
- 2.5. Определить места уязвимости АС и выбрать средства защиты информации.

Литература:

1. Доктрина информационной безопасности РФ. - сайт Правительства РФ, [www.gov.ru](http://www.gov.ru).
2. Информационные системы и технологии в экономике: Учебник. / Т.П. Барановская, В.И. Лойко, М.И. Семенов, А.И. Трубилин; Под ред. В.И. Лойко. – М.: Финансы и статистика, 2003. – 416 с.
3. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. - М.: МИФИ, 1995.
4. Галатенко В. Информационная безопасность//Открытые системы, № 4-6, 1995, № 1-4, 1996.
5. Зегжда П.Д. и др. Теория и практика обеспечения информационной безопасности. – М.: Изд-во Яхтсмен, 1996. - 192с.
6. Концепция национальной безопасности РФ. - сайт Правительства РФ, [www.gov.ru](http://www.gov.ru).
7. Медведовский И., Семьянов П., Платонов В. Атака через «INTERNET».- СПб: НПО «Мир и семья - 95», 1997.
8. Мельников В.В. Защита информации в компьютерных системах. - М.: Финансы и статистика, Электронинформ, 1997.
9. Сборник руководящих документов по защите информации от несанкционированного доступа. – М: Гостехкомиссия, 1998. – 120 с.
10. Харрис Н. CISSP. Руководство подготовки к экзамену. – М.: McGraw-Hill, 2012. – 1472с.

Разработка модели разграничения доступа к информации является одним из этапов проектирования СЗИ защищенной АС. Она предназначена для автоматизации информационных процессов в системе управления (СУ) объектом и обеспечивает повышение 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.

## 2.1. Разработать перечень защищаемых ресурсов и их критичности.

### 2.1.1. 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 до-

стуга. 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.

### 2.1.2. 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 распоряжительного документа с приложением к нему сводного перечня задач, которые планируются

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 2.1.

Таблица 2.1. 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	АРМ1	Секретно	Пользователи отдела
3	Рабочее место начальника ОО	АРМ2	Сов. секретно	Начальник и зам. начальника отдела
4	Рабочее место пользователей ОК	АРМ3	Секретно	Пользователя 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	С1	Сов. секретно	Администратор безопасности ЛВС
10	ОС Windows NT 4.0	ОС336790422	Несекретно	Администратор безопасности ЛВС
11	...			

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

### 2.2.1. 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.

### 2.2.2. 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 ин-

формационным 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 2.2. 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 2.2. Разделение ресурсов в организации

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

3	...					
---	-----	--	--	--	--	--

### 2.3. 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.

#### 2.3.1. Анализ информационной архитектуры системы

##### *2.3.1.1. 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.

##### *2.3.1.2. 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.

##### *2.3.1.3. 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.

#### *2.3.1.4. 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.

#### *2.3.1.5. 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.

### 2.3.2. 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.

#### 2.3.2.1. Определение особенностей функционирования службы

Определение особенностей функционирования службы заключается 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.

#### 2.3.2.2. 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 интерфейсы, 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 2.3.

Таблица 2.3. Защищенность информационных ресурсов организации

Элементы данных	Уровень ущерба по свойствам информации			
	Конфиденциальность	Целостность	Доступность	Защита от тиражирования
N <sub>1</sub>	Нет	Средний	Средний	Нет
N <sub>2</sub>	Высокий	Средний	Средний	Нет
N <sub>m</sub>	Низкий	Низкий	Низкий	Нет
В итоге	Высокий	Средний	Средний	Нет

#### 2.3.2.3. 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 2.4).

Таблица 2.4. 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.

#### *2.3.2.4. 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.

#### *2.3.2.5. 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.

### 2.3.2.6. 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.

### 2.3.3. 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.

#### 2.4. 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.

#### 2.5. 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.

##### *2.5.1. 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.

##### *2.5.2. 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.

### 2.5.3. 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.

#### *2.5.3.1. 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 си-



стемы 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.

#### 2.5.3.2. Побочные электромагнитные и другие излучения и наводки

Основные каналы утечки информации, возникающие за счет физических полей, можно проиллюстрировать следующей таблицей 2.5 и рисунком 2.1:

Таблица 2.5. 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.



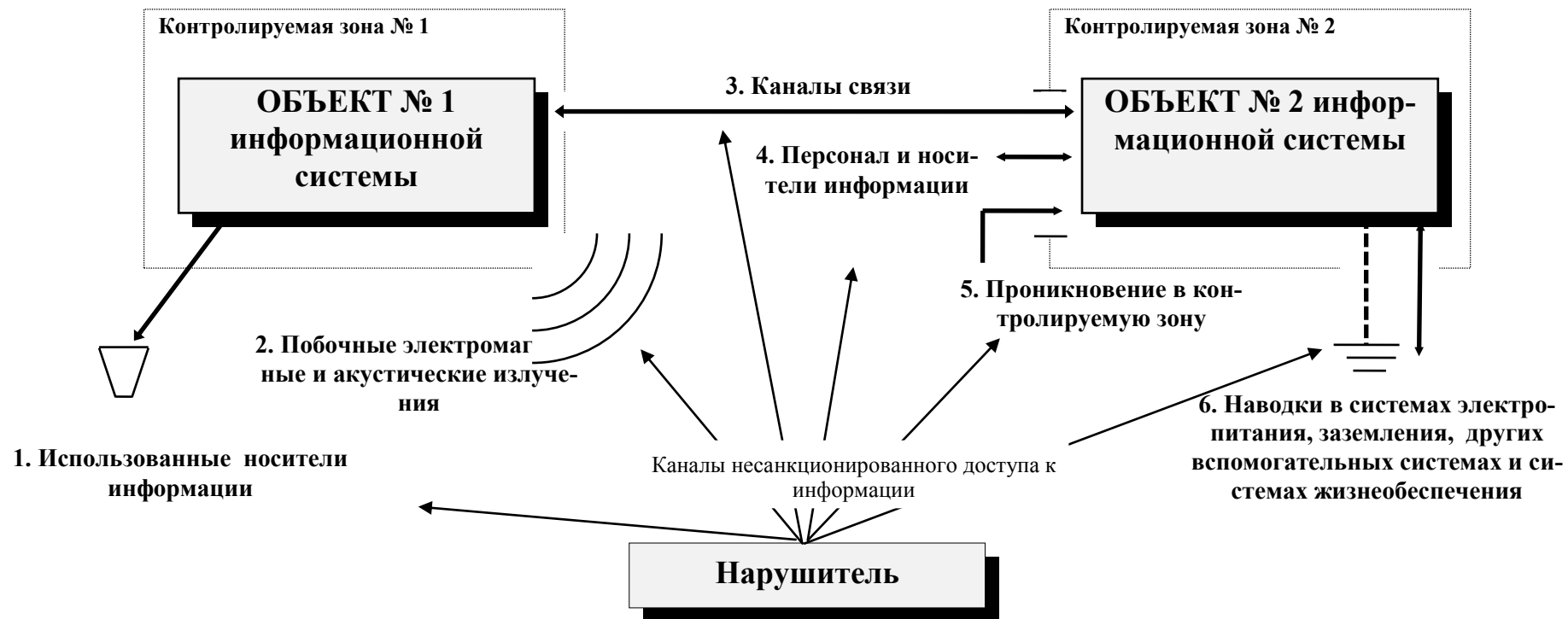


Рисунок 2.1. Информационное взаимодействие объектов и воздействие на него нарушителем

#### 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 2.6.

Таблица 2.6. 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.

#### *2.5.4.2. 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.

#### *2.5.4.3. 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.

#### 2.5.4.4. 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
<b>Общая структура системы управления</b>																					
- несколько структурных подразделений в одном здании	+			+			+			+				+			+		+		
- несколько структурных подразделений в близко расположенных зданиях		+			+			+			+				+			+		+	
- несколько территориально разнесенных зданий			+			+			+			+				+			+		+
<b>Характер информационной деятельности</b>																					
- орган государственного управления	+	+	+										+	+	+						
- государственная организация				+	+	+										+	+	+			
- кредитно-финансовое учреждение							+	+	+										+	+	+
- коммерческое предприятие										+	+	+									
<b>Уровень конфиденциальности информации</b>																					
- 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 видеозображения		+				+					+				+			+	+

## 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				
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				

### ЛЗ-03. Программирование арифметических алгоритмов шифрования (2 часа)

**Цель занятия** - Исследование и использование основных методов симметричных криптосистем для шифрования конкретных тестов.

Учебные вопросы:

- 3.1. Исследование основных методов симметричных криптосистем.
- 3.2. Использование для шифрования конкретных тестов

Литература:

1. Информационные системы и технологии в экономике: Учебник. / Т.П. Барановская, В.И. Лойко, М.И. Семенов, А.И. Трубилин; Под ред. В.И. Лойко. – М.: Финансы и статистика, 2003. – 416 с.
2. Жельников В. Криптография от папируса до компьютера. М.: АБФ, 2007. – 336 с.
3. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005. – 424 с.
4. Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, -2002.
5. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002.

#### **Введение**

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, которая определяется степенью защищенности и устойчивости как компьютерных систем в целом, так и отдельных программ.

#### **Сведения из теории**

**Криптография** – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифрованием, которые выполняются по специальным алгоритмам с помощью ключей.

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

**Криптоанализ** – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

**Кодирование** – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптосистемы разделяются на **асимметричные** и с **открытым ключом**.

В **симметричных криптосистемах** и для шифрования, и для дешифрования используется **один и тот же ключ**.

В **системах с открытым ключом** используются два ключа - **открытый** и **закрытый**, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений. Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования - расшифрования. В соответствии со стандартом ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» под **шифром** понимают совокупность обратимых



преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

- алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
- алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
- гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
- аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифрования осуществляются в рамках некоторой криптосистемы. Для **симметричной** криптосистемы характерно применение одного и того же ключа, как при шифровании, так и при расшифровании сообщений. В **асимметричных** криптосистемах для зашифрования данных используется один (общедоступный) ключ, а для расшифрования – другой (секретный) ключ.

### 3.1. Исследование основных методов симметричных криптосистем.

**Симметричные криптосистемы. Шифры перестановки.** В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение «Сегодня новый день» записывается в таблицу из 4 строк и 4 столбцов по столбцам.

Таблица 1 – Построение таблицы «Шифры перестановки».

С	Д	О	Д
Е	Н	В	Е
Г	Я	Ы	Н
О	Н	Й	Ь

Для получения шифрованного сообщения текст считывается по строкам и группируется по 4 букв: СДОД\_ЕНВЕ\_ГЯЫН\_ОНЙЬ

Несколько большей стойкостью к раскрытию обладает **метод одиночной перестановки** по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово Ваза, получим следующую таблицу

Таблица 2 – Построение таблицы «метод одиночной перестановки».

В	А	З	А					А	А	В	З
З	1	4	2					1	2	3	4
С	Д	О	Д					Д	Д	С	О
Е	Н	В	Е					Н	Е	Е	В
Г	Я	Ы	Н					Я	Н	Г	Ы
О	Н	Й	Ь					Н	Ь	О	Й

До перестановки.

После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо.

16	3	2	13			О	И	Р	Т
5	10	11	8			З	Ш	Е	Ю
9	6	7	12			–	Ж	А	С
4	15	14	1			Е	Г	О	П

Получается шифровка: ДДСО\_НЕЕВ\_ЯНГЫ\_НЬОЙ.

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются **алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок будет обратный. Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 x 3 их 36, для 4 x 4 их 576, а для 5\*5 их 14400.

Пример данного метода шифрования показан в следующих таблицах. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы:

Таблица 3 - Двойная перестановка столбцов и строк.

	2	4	1	3			1	2	3	4			1	2	3	4
4	С	Е	Г	О		4	Г	С	О	Е		1	Я	Д	Н	Н
1	Д	Н	Я	Н		1	Я	Д	Н	Н		2	Ы	О	Й	В
2	О	В	Ы	Й		2	Ы	О	Й	В		3	Н	Д	Ь	Е
3	Д	Е	Н	Ь		3	Н	Д	Ь	Е		4	Г	С	О	Е

В результате перестановки получена шифровка: ЯДННЬОЙВНДЬЕГСОЕ.

В средние века для шифрования применялись и **магические квадраты**. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

П	Р	И	Е	З	Ж	А	Ю	–	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Число магических квадратов очень резко возрастает с увеличением размера его сторон:

для таблицы 3\*3 таких квадратов -1; для таблицы 4\*4 - 880; а для таблицы 5\*5-250000.

### 3.2. Использование для шифрования конкретных тестов

#### **Порядок выполнения работы**

На любом известном Вам языке программирования написать программу шифрования и дешифрования текстового файла по вариантам:

1. Метод перестановки
2. Метод одиночной перестановки
3. Метод двойной перестановки

#### **Содержание отчета**

1. Название работы.
2. Цель работы.
3. Блок-схему алгоритма шифрования.
4. Тексты программ.

#### **Вопросы для самопроверки**

1. Цель и задачи криптографии.
2. Шифры одиночной перестановки и перестановки по ключевому слову.
3. Шифры двойной перестановки. Шифрование с помощью магического квадрата.

## ЛЗ-04. Программирование алгебраических алгоритмов шифрования (2 часа)

**Цель занятия** - исследование и использования классических методов симметричных криптосистем на базе алгебраических алгоритмов шифрования

Учебные вопросы:

- 4.1. Исследование основных методов симметричных криптосистем.
- 4.2. Использование для шифрования конкретных тестов

Литература:

1. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002.
2. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1997. – 336с.  
Информационные системы и технологии в экономике: Учебник. / Т.П. Барановская, В.И. Лойко, М.И. Семенов, А.И. Трубилин; Под ред. В.И. Лойко. – М.: Финансы и статистика, 2003. – 416 с.
3. Коблиц Н. Курс теории чисел в криптографию. – М.: Научное издательство ТВП, 2001 г.
4. Масленников А. Практическая криптография ВHV – СПб.: Петер. 2003.
5. Мельников В.В. Защита информации в компьютерных системах. - М.: Финансы и статистика, Электронинформ, 1997.
6. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. - М.: ДМК, 2000г. – 448 с.
7. Фергюсон Н. Шнайер Б. Практическая криптография. - М.: Издательский дом «Вильямс», 2005. – 424 с.
8. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф. 2002.

### 4.1. Исследование основных методов симметричных криптосистем

Для обеспечения защиты информации в настоящее время не существует какого-то одного технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптоподобных преобразований информации.

#### **Краткие сведения из теории**

**Шифры простой замены. Система шифрования Цезаря** - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на К букв.

Известная фраза Юлия Цезаря «VENI VINI VICI» – «пришел, увидел, победил», зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5\*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

**Шифры сложной замены. Шифр Гронсфельда** состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение СОВЕРШЕННО СЕКРЕТНО

Ключ 3143143143143143143

Шифровка ФПИСЬИОССАХИЛФИУСС

В шифрах многоалфавитной замены для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

Таблица 3.1. – Шифр многоалфавитной замены.

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	.....
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Таблица 3.2. – Пример 1.

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮАЕОТМГО

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

### Гаммирование

1. Процесс зашифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки  $T(0)_i$  одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков  $\Gamma(\pi)_i$  аналогичной длины

$$T(\pi)_i = \Gamma(\pi)_i + T(0)_i \quad (1)$$

где  $+$  - побитовое сложение,  $i = 1-m$ .

Процесс расшифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные  $T(0)_i = \Gamma(\pi)_i + T(\pi)_i$ .

$$T(0)_i = T(\pi)_i - \Gamma(\pi)_i$$

## 4.2. Использование для шифрования конкретных тестов

### Порядок выполнения работы

1. Основные шаги шифрования текстового файла методом гаммирования. Алгоритм описан словесно.
2. Получить от пользователя ключ, имя входного и выходного файла.
3. Инициализировать генератор случайных чисел с помощью ключа. Открыть указанные файлы.
4. Прочитать строку из файла.
5. Получить случайное число.
6. Получить ASCII-код очередного символа строки и увеличить его на случайное число, полученное на шаге 4.
7. Проверить правильность (допустимый диапазон) нового ASCII-кода.
8. В выходную строку записать очередной символ, соответствующий ASCII-коду, полученному на шаге 6.
9. Если не достигли конца входной строки, то перейти к шагу 4.
10. Записать полученную строку в выходной файл.
11. Если не достигнут конец файла, то перейти к шагу 3.
12. Закрыть файлы.
13. Алгоритм дешифрации аналогичен алгоритму шифрации за исключением того, что из ASCII – кода вычитаем 256 и проверяем больше нуля или нет.

На известном Вам языке программирования написать программу шифрования и дешифрования текстового файла. Использовать все 3 метода:

1. Шифр Гронсфелда.
2. Шифры двойной перестановки. Шифрование с помощью магического квадрата.
3. Шифр многоалфавитной замены и алгоритм его реализации.

### Содержание отчета

1. Название работы.
2. Цель работы.
3. Блок-схему алгоритма шифрования.
4. Тексты программ.

## ЛЗ-05. Контроль состояния безопасности информации (2 часа)

**Цель занятия** - изучить и практически научиться осуществлять контроль за состоянием безопасности информации.

Учебные вопросы

- 5.1. Средства ведения и анализа системных журналов ОС Windows
- 5.2. Средства контроля за процессами. Свойства процессов и управление ими
- 5.3. Анализ настройки системы разграничения доступа в среде ОС Windows

Литература:

1. Информационные системы и технологии в экономике: Учебник. / Т.П. Барановская, В.И. Лойко, М.И. Семенов, А.И. Трубилин; Под ред. В.И. Лойко. – М.: Финансы и статистика, 2003. – 416 с.

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

### 5.1. 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	Вход пользователя в систему запрещен - учетная

Идентификатор	Категория	Описание
	системы	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
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 <sup>2</sup>	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

Идентификатор	Категория	Описание
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 су-

щественным недостатком подсистемы аудита ОС Windows.

### 5.2. 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 1.** 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 2.** 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 3.** 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 Закрыть ресурс, 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 удаления. Вы можете удалиться, 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. Нажмите на кнопку 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 окна 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).

### 5.3. 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 по очереди 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 пользователей, 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-06. Исследование проблем очистки магнитных носителей**

(2 часа)

**Цель занятия** - изучить и освоить практически технологию уничтожения и восстановления файлов на магнитных носителях. Выполнить задания ЛЗ и представить результаты их выполнения преподавателю.

Учебные вопросы:

- 6.1. Восстановление удаленных файлов
- 6.2. Восстановление отформатированных дискет
- 6.3. Средства освобождения областей оперативной памяти и внешних накопителей

Литература:

1. Информационные системы и технологии в экономике: Учебник. / Т.П. Барановская, В.И. Лойко, М.И. Семенов, А.И. Трубилин; Под ред. В.И. Лойко. – М.: Финансы и статистика, 2003. – 416 с.
2. Описание программ "Крот-М" или "Terrier "

### 6.1. 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".

#### **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 А:, двумя способами:
  - выполнив поиск по ключевым словам на свободном пространстве;
  - просмотрев содержание соответствующих удаленному файлу физических секторов.
5. Просмотреть содержимое диска А: 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.

## 6.2. 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.

## 6.3. 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:» выбирать в списке диск A: и нажать кнопку [Далее].
4. На следующем экране в качестве метода стирания выбирать [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 Безопас-

ности) 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-07. Применение программных антивирусных комплексов (2 часа)

**Цель занятия** - научиться настраивать и применять антивирусные программные комплексы.

Учебные вопросы:

- 7.1. Настройка антивирусных программных комплексов
- 7.2. Применение антивирусных программных комплексов

Литература:

1. Расторгуев С. Программные методы защиты информации в компьютерах и сетях. - М.: Яхтсмен, 2014. – 154с.

### 7.1. Настройка антивирусных программных комплексов

#### **7.1.1. 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 [Пе-

реместить 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.


### 7.1.2. 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.

## 7.2. Применение антивирусных программных комплексов

### **7.2.1. 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.

### 7.2.2. 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 обновления.

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-08. Аппаратные средства опознавания пользователей (2 часа)

**Цель занятия** - исследование аппаратных средств СЗИ (электронного замка «Соболь») и освоение управления им.

Учебные вопросы:

- 8.1. Построение аппаратных средств СЗИ (электронный замок «Соболь»).
- 8.2. Управление пользователями в СЗИ (электронный замок «Соболь»).

Литература:

1. Описание электронного замка «Соболь».

### 8.1. 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.

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. Вво-



димый 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 использующейся 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.

## 8.2. 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 8.1.

- адрес *ROM BIOS*, начиная с которого в памяти компьютера будет размещаться расширение *BIOS*, содержащееся в ПЗУ платы согласно таблице 8.2.

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 8.2

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  $\surd$  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 *<Del>* и подтвердите удаление в появившемся запросе.

Для выхода из режима просмотра системного журнала и возврата к меню администратора нажмите клавишу *<Esc>*.

## **ЛЗ-09. Средства защиты несанкционированного копирования информации** (2 часа)

**Цель занятия** – исследование программных методов защиты от несанкционированного копирования информации (НСК) и анализ их работы.

Учебные вопросы:

9.1. Привязка программ к гибким и жестким магнитным дискам. Программные методы защиты от НСК: идентификация аппаратной и программной сред, идентификация исполняемого модуля.

9.2. Средства анализа и копирования защищенных дискет и взламывания защиты программ.

Литература:

1. Информационные системы и технологии в экономике: Учебник. / Т.П. Барановская, В.И. Лойко, М.И. Семенов, А.И. Трубилин; Под ред. В.И. Лойко. – М.: Финансы и статистика, 2003. – 416 с.

2. Описание программ «НОТА» и INTRUDER 2.

### 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.

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» - Nota.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 С и установкой предельной даты запуска – a.exe, в) с установкой уровня защиты 04 – b.exe, с) с привязкой к диску А 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 дискет 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 взломанный 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-10. Защита информации с помощью пароля**

(2 часа)

**Цель занятия** - исследование защиты информации с применением пароля, а также исследование методов противодействия атакам на пароль.

Учебные вопросы:

11.1. Атаки на пароль.

11.2. Проблема выбора пароля.

Литература:

1. Информационные системы и технологии в экономике: Учебник. / Т.П. Барановская, В.И. Лойко, М.И. Семенов, А.И. Трубилин; Под ред. В.И. Лойко. – М.: Финансы и статистика, 2003. – 416 с.

### **Теоретическая часть**

#### **11.1. Атаки на пароль**

На сегодняшний день пароль является наиболее приемлемым и потому наиболее часто используемым средством установления подлинности, основанным на знаниях субъектов доступа.

В любой критической системе ошибки человека-оператора являются чуть ли не самыми дорогостоящими и распространенными. В случае криптосистем, непрофессиональные действия пользователя сводят на нет самый стойкий криптоалгоритм и самую корректную его реализацию и применение.

В первую очередь это связано с выбором паролей. Очевидно, что короткие или осмысленные пароли легко запоминаются человеком, но они гораздо проще для вскрытия. Использование длинных и бессмысленных паролей безусловно лучше с точки зрения криптостойкости, но человек обычно не может их запомнить и записывает на бумажке, которая потом либо теряется, либо попадает в руки злоумышленнику. Именно из того, что неискушенные пользователи обычно выбирают либо короткие, либо осмысленные пароли, существуют два метода их вскрытия: атака полным перебором и атака по словарю.

Защищенность пароля при его подборе зависит, в общем случае, от скорости проверки паролей и от размера полного множества возможных паролей, которое, в свою очередь, зависит от длины пароля и размера применяемого алфавита символов. Кроме того, на защищенность сильно влияет реализация парольной защиты.

В связи с резким ростом вычислительных мощностей атаки полным перебором имеют гораздо больше шансов на успех, чем раньше. Кроме того, активно используются распределенные вычисления, т.е. равномерное распределение задачи на большое количество машин, работающих параллельно. Это позволяет многократно сократить время взлома.

Однако вернемся на несколько лет назад, когда вычислительной мощности для полного перебора всех паролей не хватало. Тем не менее, хакерами был придуман остроумный метод, основанный на том, что в качестве пароля человеком выбирается существующее слово или какая-либо информация о себе или своих знакомых (имя, дата рождения и т.п.). Ну, а поскольку в любом языке не более 100000 слов, то их перебор займет весьма небольшое время, и от 40 до 80% существующих паролей может быть угадано с помощью простой схемы, называемой «атакой по словарю». До 80% этих паролей может быть угадано с использованием словаря размером всего 1000 слов.

Пусть сегодня пользователи уже понимают, что выбирать такие пароли нельзя, но, видимо, никогда эксперты по компьютерной безопасности не дождутся использования таких простых и радующих душу паролей, как 34jXs5U@bTa!6;). Поэтому даже искушенный пользователь хитрит и выбирает такие пароли, как hope1, user1997, pAsSwOrD, toor, roottoor, parol, gfhjkm, asxz. Видно, что все они, как правило, базируются на осмысленном слове и некотором

простом правиле его преобразования: прибавить цифру, прибавить год, перевести через букву в другой регистр, записать слово наоборот, прибавить записанное наоборот слово, записать русское слово латинскими буквами, набрать русское слово на клавиатуре с латинской раскладкой, составить пароль из рядом расположенных на клавиатуре клавиш и т.п.

Поэтому не надо удивляться, если такой «хитрый» пароль будет вскрыт хакерами — они не глупее самих пользователей, и уже вставили в свои программы те правила, по которым может идти преобразование слов. В самых «продвинутых» программах (JohnTheRipper, PasswordCrackinglibrary) эти правила могут быть программируемыми и задаваться с помощью специального языка самим хакером.

Приведем пример эффективности такой стратегии перебора. Во многих книгах по безопасности предлагается выбирать в качестве надежного пароля два осмысленных слова, разделенных некоторым знаком (например, good!password). Подсчитаем, за сколько времени в среднем будут сломаны такие пароли, если такое правило включено в набор программы-взломщика (пусть словарь 10000 слов, разделительными знаками могут быть 10 цифр и 32 знака препинания и специальных символа, машина класса Pentium со скоростью 15000 паролей/сек):

$$10000 \cdot (32 + 10) \cdot 10000 / 15000 \cdot 2 = 140000 \text{ секунд или менее 1.5 дня!}$$

Чем больше длина пароля, тем большую безопасность будет обеспечивать система, так как потребуются большие усилия для его отгадывания. Это обстоятельство можно представить в терминах ожидаемого времени раскрытия пароля или ожидаемого безопасного времени. *Ожидаемое безопасное время ( $T_b$ ) — половина произведения числа возможных паролей и времени, требуемого для того, чтобы попробовать каждый пароль из последовательности запросов.*

Если после каждой неудачной попытки подбора автоматически предусматривается десятисекундная задержка, то безопасное время резко увеличивается.

Поэтому при использовании аутентификации на основе паролей защищенной системой должны соблюдаться следующие правила:

- а) не позволяются пароли меньше 6—8 символов;
- б) пароли должны проверяться соответствующими контроллерами;
- в) символы пароля при их вводе не должны появляться в явном виде;
- г) после ввода правильного пароля выдается информация о последнем входе в систему;
- д) ограничивается количество попыток ввода пароля;
- е) вводится задержка времени при неправильном пароле;
- ж) при передаче по каналам связи пароли должны шифроваться;
- з) пароли должны храниться в памяти только в зашифрованном виде в файлах, недоступных пользователям;
- и) пользователь должен иметь возможность самому менять пароль;
- к) администратор не должен знать пароли пользователей, хотя может их менять;
- л) пароли должны периодически меняться;
- м) устанавливаются сроки действия паролей, по истечении которых надо связаться с администратором.

## 11.2. Проблема выбора пароля

Выбор длины пароля в значительной степени определяется развитием технических средств, их элементной базы и ее быстродействием. В настоящее время широко применяются многосимвольные пароли, где  $S > 10$ . В связи с этим возникают вопросы: как и где его хранить и как связать его с аутентификацией личности пользователя? На эти вопросы отвечает комбинированная система паролей, в которой код пароля состоит из двух частей. Первая часть состоит из 3—4-х десятичных знаков, если код цифровой, и более 3—4-х, если код буквенный, которые легко запомнить человеку. Вторая часть содержит количество знаков, определяемое требованиями к защите и возможностями технической реализации системы, она помещается на физическом носителе и определяет ключ-пароль, расчет длины кода которого ведется по указанной выше методике. В этом случае часть пароля будет недоступна для нарушителя.

Однако при расчете длины кода пароля не следует забывать о том, что при увеличении длины пароля нельзя увеличивать периодичность его смены. Коды паролей необходимо менять обязательно, так как за большой период времени увеличивается вероятность их перехвата путем прямого хищения носителя, снятия его копии, принуждения человека. Выбор периодичности необходимо определять из конкретных условий работы системы, но не реже одного раза в год. Причем желательно, чтобы дата замены и периодичность должны носить случайный характер.

Для проверки уязвимости паролей используются специальные контроллеры паролей. Например, известный контроллер Кляйна, осуществляет попытки взлома пароля путем проверки использования в качестве пароля входного имени пользователя, его инициалов и их комбинаций, проверки использования в качестве пароля слов из различных словарей, начиная от наиболее употребительных в качестве пароля, проверки различных перестановок слов, а также проверки слов на языке пользователя—иностранца. Проверка паролей в вычислительных сетях с помощью контроллера Кляйна показала довольно высокие результаты — большинство пользователей используют простые пароли. Показателен пример, когда контроллер Кляйна позволил определить 100 паролей из 5 символов, 350 паролей из 6 символов, 250 паролей из 7 символов и 230 паролей из 8 символов.

Приведенный анализ позволяет сформулировать следующие правила снижения уязвимости паролей и направленные на противодействие известным атакам на них:

- расширяйте применяемый в пароле алфавит — используйте прописные и строчные буквы латинского и русского алфавитов, цифры и знаки;
- не используйте в пароле осмысленные слова;
- не используйте повторяющиеся группы символов;
- не применяйте пароли длиной менее 6—8 символов, так как запомнить их не представляет большого труда, а пароль именно нужно запоминать, а не записывать. По той же причине не имеет смысла требовать длину неосмысленного пароля более 15 символов, так как запомнить его нормальному человеку практически невозможно;
- не используйте один и тот же пароль в различных системах, так как при компрометации одного пароля страдают все системы;
- проверяйте пароли перед их использованием контроллерами паролей.

Для составления пароля можно дать рекомендации, которыми пользоваться надо очень осторожно:

- выберите несколько строк из песни или поэмы (только не те, которые Вы повторяете первому встречному) и используйте первую (или вторую) букву каждого слова — при этом пароль должен иметь большую длину (более 15 символов), иначе нужно менять регистры букв, применять латинские буквы вместо русских или наоборот, можно вставлять цифры и знаки;
- замените в слове из семи—восьми букв одну согласную и одну или две гласных на знаки или цифры. Это даст вам слово-абракадабру, которое обычно произносимо и поэтому легко запоминается. Подведем итог:

**Что такое плохой пароль:**

- Собственное имя;
- Слово, которое есть в словаре;
- Идентификатор, присвоенный Вам какой-нибудь системой, или любые его вариации;
- Дата рождения;
- Повторенный символ (например:AAA);
- Пароль меньше 6 символов;
- Пароль, установленный Вам чужим человеком;
- Пароль, состоящий из символов соседствующих на клавиатуре (например: QWERTY или ЙЦУКЕ);
- Пароль состоящий из паспортных данных: персональный номер, номер водительских прав и т.д.

**Что такое хороший пароль:**

- Бессмысленная фраза;

- Случайный набор символов вперемешку с буквами.

### **Порядок работы с программами вскрытия паролей.**

В данной лабораторной работе используется программный продукт для вскрытия закрытых паролем архивов: Advanced ZIP PasswordRecovery.

### **Работа с программами взлома на примере AZPR**

Программа AZPR используется для восстановления забытых паролей ZIP-архивов. На сегодняшний день существует два способа вскрытия паролей: перебор (bruteforce) и атака по словарю (dictionary-basedattack).

Панель управления:

- кнопки Открыть и Сохранить позволяют работать с проектом, в котором указан вскрываемый файл, набор символов, последний протестированный пароль. Это позволяет приостанавливать и возобновлять вскрытие.

- кнопки Старт и Стоп позволяют соответственно начинать и заканчивать подбор пароля.

- кнопка Набор позволяет задать свое множество символов, если известны символы, из которых состоит пароль.

- кнопка Справка выводит помощь по программе.

- кнопка О AZPR выводит информацию о программе.

- кнопка Выход позволяет выйти из программы

Рассмотрим возможности программы:

Выбирается архив для вскрытия и тип атаки.

Выбираются параметры работы:

- Закладка Набор

Программа позволяет выбрать область перебора (набор символов). Это значительно сокращает время перебора. Можно использовать набор пользователя, заданный с помощью кнопки Набор. Можно ограничить количество тестируемых паролей, задав начальный пароль. В случае если известна часть пароля, очень эффективна атака по маске. Нужно выбрать соответствующий тип атаки, после этого станет доступным поле маска. В нем нужно ввести известную часть пароля в виде P?s?W?r? , где на месте неизвестных символов нужно поставить знак вопроса. Можно использовать любой другой символ, введя его в поле символ маски.

- Закладка Длина

Позволяет выбрать длину пароля.

- Закладка Словарь

Позволяет выбрать файл-словарь. Выбирайте файл English.dic, он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

- Закладка Автосохранение

Можно выбрать имя файла для сохранения результатов работы и интервал автосохранения.

- Закладка Опции

Выбирается приоритет работы (фоновый или высокий), интервал обновления информации о тестируемом в данный момент пароле. Увеличение интервала повышает быстродействие, но снижает информативность. Также можно установить режим ведения протокола работы и возможность минимизации программы в tray (маленькая иконка рядом с часами).

## **11.3. Порядок выполнения работ**

### **Проведение атаки перебором (bruteforceattack)**

1.Используя программу для вскрытия паролей произвести атаку на зашифрованный файл. Область перебора — все печатаемые символы, длина пароля от 1 до 4 символов. Проверить правильность определенного пароля, распаковав файл и ознакомившись с его содержимым.

2.Выполнив пункт 1, сократить область перебора до фактически используемого (например если пароль 6D1A — то выбрать прописные английские буквы и цифры). Провести повторное вскрытие. Сравнить затраченное время.

### **Проведение атаки по словарю (dictionaryattack)**

1.Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например love, god, table, admin и т.д.). Провести атаку по словарю. Для этого выбрать вид атаки и в закладке Словарь выбрать файл English.dic. Он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

2.Попытаться определить пароль методом прямого перебора. Сравнить затраченное время.

## ЗАКЛЮЧЕНИЕ

В заключении дадим методологические советы студентам, осваивающим практику применения теории информационной безопасности в своей будущей специальности.

Важная задача практического освоения технологий эффективного использования защиты информации в профессиональной деятельности специалистов разного профиля может быть успешно решена только в том случае, если на основе теоретических и прикладных положений теории защиты информации обучаемые освоят работу по ее разделам

- организационно-правовой,
- инженерно-технической,
- аппаратно-программной и
- криптографической

практически.

Они должны научиться реализовать свои знания в сфере ЗИ на уровне **умений** (результативного применения всего арсенала средств и методов защиты информации в АИС), а, еще лучше, **навыков** (автоматической реализации умений в своей практической деятельности), позволяющих им успешно конкурировать на рынке труда в сфере информационных систем и технологий). Для этого им надо без усталости работать с этими средствами и методами, совершенствовать умения и навыки их профессионального использования по специальности. Именно этому и способствует качественное выполнение каждым обучаемым всех 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. Харрис Н. CISSP. Руководство подготовки к экзамену. – М.: McGraw-Hill, 2012. – 1472с.

### *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, 2014. – 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.
8. Меры защиты информации в государственных информационных системах: Методический документ. /утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г./ <http://www.garant.ru/products/ipo/prime/doc/70491518/>

### *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, 2013. – 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, 2010. – 98с.
12. Зима В. Компьютерные сети и защита передаваемой информации. /В. Зима, А. Молдовян., Н. Молдовян. – СПб.: СПбГУ, 2012. – 198с.
13. Мельников В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 2007. – 157с.
14. Расторгуев С. Программные методы защиты информации в компьютерах и сетях. - М.: Яхтсмен, 2014. – 154с.
15. Расторгуев С. Информационная война. - М.: Радио и связь, 1998. - 416с.
16. Трубочев А.П. и др. Оценка безопасности информационных технологий. - М.: Издательство СИП РИА, 2013. - 356с.
17. Шангин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: ИД "ФОРУМ": ИНФРА-М, - 2008. – 416 с.
18. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический проект; Гаудеамус, 2012, - 544с.



## ПРИЛОЖЕНИЯ

### Приложение-1. Программа СРС по дисциплине

#### 1. Содержание самостоятельной работы

Самостоятельная работа студента (СРС) по дисциплине «Защита информации» (ЗИ) осуществляется путем освоения будущими инженерами тем и вопросов учебного курса, не включенных в лекционный курс и лабораторные занятия. При выполнении заданий СРС студент обязан самостоятельно изучить дополнительные учебно-методические материалы по защите информации и выполнить задания, подготовленные ведущими преподавателями кафедры компьютерных технологий КубГАУ с учетом особенностей специальности 230201.65 – «Информационные системы и технологии».

Цель СРС – самостоятельное изучение будущими бакалаврами теоретических и прикладных разделов ЗИ, дающих углубленное представление о механизмах проектирования и использования систем защиты информации (СЗИ), обеспечивающего эффективное применение информационных систем и технологий (ИТиТ).

Задачи СРС – самостоятельное освоение студентом под руководством преподавателя перечисленных ниже вопросов-заданий по тематике дисциплины «Защита информации».

В результате самостоятельного выполнения этой работы бакалавры должны:

#### **знать**

- функциональные процессы в системах защиты ИСиТ;
- средства, способы и методы ЗИ, обеспечивающие благоприятные условия для создания и эффективного применения технологии автоматизированного сбора, хранения, анализа, обработки и передачи информации;

#### **уметь**

- применять полученные знания при ЗИ в автоматизированном управлении процессами решения функциональных задач и обработке информации;

#### **обладать навыками**

- проектирования и использования СЗИ в автоматизированном управлении технологическими и социальными процессами;
- выполнения расчетов и подготовки необходимой документации по информационной безопасности в рамках своей профессиональной деятельности на компьютере;
- поиска необходимой сведений по защите информации в отраслевых, национальных и мировых базах знаний и данных.

#### 2. Виды и объём самостоятельной работы студента по ИБ

Вид самостоятельной работы	Всего часов	Форма контроля
1. Самостоятельное углубленное изучение отдельных тем (вопросов) ИБ	50	ТК, От
2. Подготовка и защита рефератов по ЗИ в рамках индивидуальных заданий для студентов	4	Зр, Дк
3. Подготовка и выступление с докладом, научным сообщением, статьей на семинарах и конференциях по ЗИ	4	Пп, ТК
4. Проведение компьютерного патентного поиска сведений по дисциплине	4	Зр, Дк
5. Выполнение курсовых работ, НИРС по ЗИ	64	От, С
7. Другие виды самостоятельной работы (подготовка к зачету и др.)	6	От, С
Общий объём:	132	

**Примечание.** При проведении ЛЗ и СРС используются следующие виды отчетности:

- Дк – подготовка и выступление с докладом, рефератом, научной статьей;
- Зр – защита реферата, представление доклада, научной работы по НИРС;
- От – отчет студента по курсовой работе, самостоятельно отрабатываемому вопросу;
- Пп – представление результатов патентного поиска;
- С – собеседование;
- ТК – текущий контроль.

### 3. Темы (вопросы), выносимые на СРС по ЗИ и рекомендуемая литература

№ п/п	Тема (вопрос), выносимый на самостоятельную работу студентов	Литература	
		основная	допол-ная
1.	Традиционные ИТ в экономике и обеспечение ЗИ	[1], [3]	[8], [12]
2.	Особенности использования СЗИ в экономике	[1]-[3]	[14]-[16]
3.	Сходство и различие понятийных аппаратов информатики и ЗИ. Пути их сближения при проектировании и эксплуатации отраслевых АИС	[4]	[6]
4.	СЗИ, их использование в профессиональной деятельности бакалавров	[1]-[3]	[5], [11]
5.	Методология и методы конструирования СЗИ в экономических АИС.	[1], [4]	[5]-[6]
6.	Особенности информационных моделей ЗИ, реализуемых в экономике	[2]	[6], [10], [14]
7.	СЗИ обеспечивающие функционирование и развитие АИС	[1]-[2], [4]	[8]-[9], [12]
8.	Особенности применения организационно-правовых средств и методов ЗИ в экономической деятельности.	[1]-[2], [4]	[8]-[9], [12]
9.	Аппаратно-программные средства ЗИ и использование и совершенствования.	[2]	[11], [13]-[18]
10.	Функционирование и развитие криптографических средств и методов ЗИ	[1], [3]	[7], [13], [17]
11.	Реализации базовой информационной технологии (БИТ) и пути обеспечения ЗИ в ней.	[3]	[15],
12.	Специфика механизма реализации ЗИ в БИТ и его совершенствование	[1], [3]	[13] [17],
13.	Адаптивные СЗИ и специфика их применения в экономике	[1], [3]	[18]
14.	Автоматизированный системно-когнитивный анализ (АСК-анализ) как перспективная основа совершенствования СЗИ	[3]	[17]

Примечание. Номера рекомендуемой литературы (основной и дополнительной) соответствуют номерам в списке литературы к данному практикуму.

## Приложение 2. Перечень УММ, по дисциплине

Пособия и учебно-методические материалы (УММ) кафедры КТС используемые по дисциплине «Защита информации» по направлению 230400.62 – Информационные системы и технологии:

1. Защита информации: Справочник нормативных документов для бакалавров. / В.Н. Лаптев, С.В. Лаптев. – Краснодар: КубГАУ, 2014. - 100с.
2. Лаптев В.Н. Защита информации: Курс лекций. – Краснодар: КубГАУ, 2014. – 186 с.
3. Лаптев В.Н. Защита информации: Методические рекомендации по выполнению курсовых работ. – Краснодар: КубГАУ, 2014. – 48 с.
4. Лаптев В.Н. Защита информации: Презентации лекций – Краснодар: КубГАУ, 2014.

УММ по дисциплине «Защита информации»:

1. Слайды и плакаты кафедры КТС КубГАУ с учебными и графическими материалами (фрагменты презентаций лекций по ЗИ).
2. Раздаточный дидактический материал по учебному курсу
3. Конспекты лекций и рабочие тетради обучающихся.

### **Приложение-3. Программное обеспечение, используемое на ЛЗ**

по дисциплине «Защита информации»

1. Универсальный интегрированный пакет для офиса Microsoft Office 2000, Professional Edition, содержащий программ:
  - 1.1. MS Word 2000 – текстовый процессор;
  - 1.2. MS Excel 2000 – табличный процессор (электронная таблица);
  - 1.3. MS Access 2000 – система управления базой данных (СУБД);
  - 1.4. MS PowerPoint 2000 – пакет демонстрационной графики (презентаций);
  - 1.5. MS Outlook 2000 – пакет планирования заданий;
  - 1.6. Internet Explorer 5 - обозреватель Internet
  - 1.7. Publisher – издательская программа;
  - 1.8. FrontPage 2000 – редактор Web–страниц;
  - 1.9. PhotoDraw – графический редактор;
  - 1.10. Small Business Nools – инструмент для ведения малого бизнеса.
2. Операционная системы:
  - 2.1. Windows 95/98/2000.
3. Файл-менеджеры:
  - 3.1. Norton Commander (NC);
  - 3.2. Windows Commander 5.0;
4. Пакеты антивирусных программ:
  - 4.1. DoctorWeb;
  - 4.3. AVP.
5. Программы-архиваторы:
  - 5.2. ZIP
  - 5.2. WinRAR.
6. Пакет сервисных программ Norton Utilities 4.
7. Интегральная среда программирования Borland-Pascal.
8. Среда визуального программирования Delphi 5

**Лаптев Владимир Николаевич  
Лаптев Сергей Владимирович  
Параскевов Александр Владимирович**

**ЗАЩИТА ИНФОРМАЦИИ**

**Практикум для бакалавров**