Автономная некоммерческая организация среднего профессионального образования

«УРАЛЬСКИЙ ПРОМЫШЛЕННО-ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ»

**Методические указания**

**к практическим занятиям**

по дисциплине

**Основы информационной безопасности**

**Укрупненная группа: 09.00.00** Информатика и вычислительная техника

**Специальность:** 09.02.03 Программирование в компьютерных системах

2016

|  |  |
| --- | --- |
| Одобрена цикловой комиссией  информатики и вычислительной техники  Председатель комиссии  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ О. Г. Максимова  Протокол  от « » \_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_г. | Методические указания разработаны на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования, входящей в состав укрупненной группы специальностей 09.00.00 «Информатика и вычислительная техника» 09.02.03 «Программирование в компьютерных системах»  *УТВЕРЖДАЮ*  Заместитель директора по  учебной работе АН ПОО «Уральский промышленно-экономический техникум»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Н.Б. Чмель  « » \_\_\_\_\_\_\_\_\_\_\_\_ 201 \_\_ г. |

Разработчик: **Максимова О.Г.** преподаватель спецдисциплин

АН ПОО «Уральский промышленно-экономический техникум»

Содержание

[Пояснительная записка 4](#_Toc479693245)

[Лабораторная работа 1 Изучение политики безопасности операционной системы Windows 7 6](#_Toc479693246)

[Лабораторная работа 2 Управление шаблонами безопасности в Windows 7 12](#_Toc479693247)

[Лабораторная работа 3 Разграничение полномочий и доступа к объектам операционной системы Unix 16](#_Toc479693248)

[Лабораторная работа 4 Настройка параметров аутентификации Windows 7 18](#_Toc479693249)

[Лабораторная работа 5 Назначение прав пользователей при произвольном управлении доступом в Windows 7 23](#_Toc479693250)

[Лабораторная работа 6 Настройка параметров регистрации и аудита в Windows 7 29](#_Toc479693251)

[Практическая работа 1 Методы криптографического преобразования данных 36](#_Toc479693252)

[Лабораторная работа 7 Использование функций криптографического интерфейса (CryptoAPI) операционной системы Windows для защиты информации. 40](#_Toc479693253)

[Лабораторная работа 8 Антивирусные программные комплексы 64](#_Toc479693254)

[Лабораторная работа 9 Восстановление зараженных файлов. Профилактика проникновения «троянских программ» 84](#_Toc479693255)

[Список рекомендуемой литературы 89](#_Toc479693256)

# Пояснительная записка

Программа учебной дисциплины «Основы информационной безопасности» является вариативной частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности среднего профессионального образования 09.02.03 «Программирование в компьютерных системах», входящей в состав укрупненной группы специальностей «Информатика и вычислительная» техника.

Дисциплина входит в общепрофессиональный цикл вариативной части.

Основной целью изучения дисциплины является формирование знаний об объектах и задачах защиты компьютерных систем, способах и средствах нарушения информационной безопасности, о принципах и подходах к решению задач защиты информации; а также формирование умений по применению современных технологий, выбора средств и инструментов защиты информации для построения современных защищенных информационных систем в соответствии с действующим законодательством.

В результате освоения учебной дисциплины обучающийся должен уметь:

* выбирать средства обеспечения информационной безопасности информационной системы современного предприятия;
* ограничивать использование ресурсов компьютера на основе раздельного доступа пользователей в операционную систему;
* организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа;
* организовывать безопасную работу в Интернет и отправку почтовых сообщений в глобальной сети;
* использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов;
* проводить базовые работы по профилактике нарушений информационной безопасности и построению защищенных информационных систем с использованием стандартных аппаратно­-программных решений.

В результате освоения учебной дисциплины обучающийся должен знать:

* вопросы административного и нормативно-правового обеспечения защиты информации
* основные системы защиты информации в России и в ведущих зарубежных странах;
* основные программно-аппаратные средства и методы защиты информации в компьютерных системах

Содержание дисциплины должно быть ориентировано на подготовку обучающихся по базовой и углубленной подготовке к освоению профессиональных модулей ОПОП по специальности «Программирование в компьютерных системах» и овладению профессиональными компетенциями (ПК):

* ПК 1.1. Выполнять разработку спецификаций отдельных компонент.
* ПК 1.2. Осуществлять разработку кода программного продукта на основе готовых спецификаций на уровне модуля.
* ПК 2.4. Реализовывать методы и технологии защиты информации в базах данных
* ПК 3.4. Осуществлять разработку тестовых наборов и тестовых сценариев. В результате освоения дисциплины у обучающихся по базовой подготовке формируются общие компетенции (ОК):
* ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
* ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
* ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
* ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
* ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.
* ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
* ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.
* ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
* ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
* ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

В рабочей программе дисциплины предусмотрено 20 часов практических и лабораторных занятий.

# Лабораторная работа 1 Изучение политики безопасности операционной системы Windows 7

**Цель занятия**: Изучить политику безопасности операционной системы Windows 7

**Норма времени**: 2 часа

**Методическое обеспечение:** методические указания к практической работе

**Теоретические сведения**

Операционная система Windows 7 создана на основе принципов безопасности Windows Vista, отвечает пожеланиям пользователей о создании более удобной и управляемой системы и содержит усовершенствования безопасности, необходимые для защиты данных в условиях быстро меняющейся структуры угроз. Самые значительные улучшения безопасности в Windows 7 рассматриваются в четырех разделах.

1.  Безопасная платформа. В основе Windows 7 лежат усовершенствования системы безопасности, впервые представленные в Windows Vista. Кроме того, она отвечает пожеланиям пользователей о создании более удобной и управляемой системы.

2.  Обеспечение безопасности универсального доступа. Windows 7 предоставляет соответствующие элементы управления безопасностью, поэтому пользователи в любое время из любого места могут обращаться к данным, необходимым для работы.

3.  Защита пользователей и инфраструктуры. Windows 7 обеспечивает гибкую защиту от вредоносных программ и вторжений, поэтому пользователи получают нужное сочетание безопасности, контроля и продуктивности.

4.  Защита данных от неавторизованного просмотра. Windows 7 расширяет технологию шифрования диска BitLocker™ для обеспечения защиты данных, хранящихся на переносных носителях (например, USB-устройствах флэш-памяти, жестких дисках USB), поэтому только авторизованные пользователи смогут считать данные даже в том случае, если носитель был украден, потерян или используется неправильно.

**Безопасная платформа.**

Фундаментальные возможности безопасности:

     защита от исправления ядра;

     ограниченный режим работы служб;

     предотвращение выполнения данных;

     случайное распределение адресного пространства;

     уровни целостности по-прежнему обеспечивают улучшенную защиту от вредоносных программ и атак.

 Эта операционная система соответствует требованиям Common Criteria для получения сертификата Evaluation Assurance Level 4 и соответствия стандарту FIPS 140-2. Опираясь на надежную платформу безопасности Windows Vista, Windows 7 вносит значительные улучшения в основные технологии защиты аудита событий и управления учетными записями пользователей.

**Усовершенствованный аудит.**

Windows 7 предоставляет усовершенствованные возможности аудита, упрощающие соблюдение нормативных и производственных требований: в том числе реализован упрощенный подход к управлению конфигурациями аудита, а выполняемые в организации задачи описаны с большей наглядностью. Например, Windows 7 помогает получить четкое представление о том, кто может получить доступ к конкретной информации, почему пользователю было отказано в доступе к определенным данным, а также узнать обо всех изменениях, внесенных пользователем или группой.

**Поддержка устройств безопасности.**

Windows 7 упрощает процесс подключения устройств безопасности к ПК и управления ими, а также предоставляет легкий доступ к общим задачам, связанным с использованием устройств. Еще никогда использование устройств безопасности не было настолько простым: при первоначальной установке и при ежедневной работе.

**Устройства хранения с усиленной безопасностью.**

Широкое использование USB-устройств флэш-памяти и других личных устройств хранения влечет за собой сомнения в безопасности данных на этих устройствах. Однако некоторым пользователям не требуются возможности полного шифрования данных BitLocker To Go™. Windows 7 поддерживает защиту с помощью паролей и проверку подлинности на основе сертификатов для USB-устройств хранения, соответствующих стандарту IEEE 1667. Для сохранения конфиденциальности данных можно использовать возможность защиты паролей, реализованную в устройствах защиты, поддерживающих стандарт IEEE 1667.

**Устройства хранения с усиленной безопасностью.**

Широкое использование USB-устройств флэш-памяти и других личных устройств хранения влечет за собой сомнения в безопасности данных на этих устройствах. Однако некоторым пользователям не требуются возможности полного шифрования данных BitLocker To Go™. Windows 7 поддерживает защиту с помощью паролей и проверку подлинности на основе сертификатов для USB-устройств хранения, соответствующих стандарту IEEE 1667. Для сохранения конфиденциальности данных можно использовать возможность защиты паролей, реализованную в устройствах защиты, поддерживающих стандарт IEEE 1667.

**Обеспечение безопасности универсального доступа.**

Windows 7 предоставляет соответствующие элементы управления безопасностью, поэтому пользователи в любое время из любого места могут обращаться к данным, необходимым для работы. Наряду с полной поддержкой существующих технологий (например, защиты сетевого доступа) Windows 7 предоставляет более гибкий брандмауэр, поддержку безопасности DNS и совершенно новую концепцию удаленного доступа.

**Поддержка DNSSec.**

DNS — это основной протокол, поддерживающий большинство ежедневных выполняемых в Интернете задач, включая доставку электронной почты, просмотр веб-страниц и обмен сообщениями. Однако следует отметить, что система DNS была разработана более трех десятков лет назад без учета современных угроз безопасности. Расширения безопасности DNS (DNSSEC) — это набор расширений DNS, предоставляющих службы безопасности, необходимые для работы в Интернете. В соответствии с требованиями документов RFC 4033, 4034 и 4035 система Windows 7 поддерживает DNSSEC, обеспечивая уверенность организаций в подлинности записей имен доменов и предоставляя защиту от вредоносных манипуляций.

**Наличие нескольких активных политик брандмауэра.**

Политика межсетевого экрана в системе Windows Vista основана на типе установленного сетевого подключения: домашнем, рабочем, общем или доменном (этот тип является скрытым). Однако, если пользователь, подключенный к Интернету через «домашнюю» сеть, использует виртуальную частную сеть для доступа в корпоративную, то это может создать серьезные проблемы безопасности. В таком случае соответствующие настройки брандмауэра для доступа к корпоративной сети не могут быть применены, поскольку тип сети (и, следовательно, параметры брандмауэра) уже был задан на основе первой сети, к которой подключен пользователь.

Windows 7 устраняет эту проблему за счет поддержки нескольких политик активного брандмауэра, позволяющих пользователям ПК получать и применять сведения о профиле брандмауэра домена вне зависимости от других сетей, к которым может быть подключен ПК. Благодаря этим возможностям, которые относятся к числу основных функций, запрашиваемых корпоративными клиентами, ИТ-специалисты могут упростить политики подключения и безопасности, поддерживая единый набор правил для удаленных клиентов и для клиентов, физически подключенных к корпоративной сети.

**DirectAccess.**

Благодаря Windows 7 работать вне офиса становится все проще. С помощью DirectAccess удаленные пользователи могут обращаться к корпоративной сети в любое время при наличии интернет-соединения, без необходимости выполнения дополнительных действий по установке VPN-подключения. Это увеличивает производительность сотрудников. DirectAccess предоставляет ИТ-специалистам более защищенную и гибкую инфраструктуру корпоративной сети для удаленного обновления пользовательских ПК и управления ими. DirectAccess упрощает управление ИТ-ресурсами за счет ввода постоянно управляемой инфраструктуры, в которой компьютеры, находящиеся в сети и вне ее, поддерживаются в работоспособном и обновленном состоянии.

С помощью DirectAccess ИТ-специалисты могут более точно контролировать сетевые ресурсы, к которым обращаются пользователи. Например, для управления доступом удаленных пользователей к приложениям предприятия можно использовать параметры групповой политики. DirectAccess отделяет интернет-трафик от доступа к ресурсам внутренней сети, поэтому пользователи могут обращаться на общедоступные веб-сайты, не создавая дополнительный трафик в сети предприятия. Кроме того, компонент DirectAccess поддерживает отраслевые стандарты (например, протоколы IPv6 и IPsec), обеспечивая защиту и безопасность корпоративного обмена данными.

**Защита пользователей и инфраструктуры.**

Windows 7 обеспечивает гибкую защиту от вредоносных программ и вторжений, поэтому пользователи могут получить нужное соотношение безопасности, контроля и продуктивности. Основными усовершенствованиями системы безопасности являются компонент AppLocker™ и браузер Internet Explorer® 8, которые обеспечивают новый стандарт защиты операционной системы от вторжения вредоносных программ в Windows 7.

**AppLocker.**

Политики управления приложениями в системе Windows 7 используются совместно со средством AppLocker — гибким и простым в управлении механизмом, позволяющим ИТ-специалистам указывать программы и компоненты, которые могут выполняться на настольных системах. Кроме того, пользователи получают возможность работать с приложениями, установочными программами и сценариями, повышающими их производительность. В итоге ИТ-специалисты могут провести в организации стандартизацию приложений, что обеспечивает безопасность и совместимость, а также улучшает производительность.

AppLocker предоставляет простые и эффективные структуры правил и вводит правила издателя: правила на основе цифровых подписей приложений. Правила издателя позволяют создавать правила, которые сохраняются после обновления приложений за счет возможности указания версии приложения в качестве атрибута. Например, в организации можно создать правило, разрешающее выполнение программы Acrobat Reader всех версий позднее 9.0, если они подписаны издателем ПО Adobe. Когда компания Adobe выпустит обновление программы Acrobat, его можно будет безопасно развернуть, не создавая еще одно правило для новой версии приложения.

**Internet Explorer 11.**

Internet Explorer 11 обеспечивает улучшенную защиту от угроз безопасности и конфиденциальности, включая возможность определения ненадежных веб-сайтов и блокировку загрузки вредоносных программ. Защита усилена благодаря возможности просматривать веб-страницы без сохранения данных на общедоступном компьютере, а также за счет расширенной настройки параметров и контроля того, каким образом веб-сайты могут отслеживать действия пользователя. В Internet Explorer 11 улучшена систему ограничений для элементов управления ActiveX ® и усовершенствовано управление надстройками. Веб-браузер обладает повышенной надежностью, которая обеспечивается функцией автоматизированного восстановления после сбоя и восстановления вкладок, а также расширенной поддержкой специальных возможностей.

**Защита данных от несанкционированного просмотра.**

Windows 7 содержит технологии защиты данных, доступные в Windows Vista: система поддерживает шифрованную файловую систему (EFS), встроенную технологию служб управления правами Active Directory® и компоненты точного контроля USB-портов. Наряду с обновленными версиями этих технологий в Windows 7 представлено несколько значительных усовершенствований популярной технологии шифрования диска BitLocker.

**BitLocker и BitLocker To Go.**

Windows 7 решает все более актуальную проблему утечки данных с помощью возможностей управления и обновлений развертывания технологии шифрования диска BitLocker и вводом нового средства BitLocker To Go, обеспечивающего улучшенную защиту от раскрытия и кражи данных за счет расширения поддержки BitLocker на съемные устройства хранения. Расширенная поддержка BitLocker для томов данных FAT затрагивает широкий диапазон устройств и форматов дисков, включая USB-устройства флэш-памяти и съемные диски. Это позволяет пользователям развертывать BitLocker при необходимости обеспечения защиты данных.

Во время поездок с переносным компьютером, обмена большими файлами с надежным партнером или работы дома защита устройств с помощью BitLocker гарантирует, что данные смогут прочесть только авторизованные пользователи даже в том случае, если носитель украден, потерян или неправильно используется. Защита BitLocker проста в развертывании, интуитивно понятна конечному пользователю, соответствует нормативным требованиям и обеспечивает должную безопасность данных.

С помощью BitLocker To Go администраторы могут контролировать использование съемных устройств хранения, а также устанавливать необходимый уровень защиты. Администраторы сделать защиту данных обязательной на любом съемном устройстве хранения, в которое пользователи будут записывать данные, разрешив использование незащищенных устройств в режиме с доступом только для чтения. Кроме того, существуют специальные политики, требующие использования соответствующих паролей, смарт-карт или учетных данных пользователя домена для работы с защищенным съемным устройством хранения. Кроме того, BitLocker To Go обеспечивает настраиваемую поддержку съемных устройств с возможностью чтения в старых версиях Windows, позволяя более безопасно обмениваться файлами с пользователями, по-прежнему работающими с ОС Windows Vista и Windows XP.

Созданная на основе принципов безопасности Windows Vista®, ОС Windows 7 содержит улучшенные функции безопасности, дающие пользователям уверенность в надежной защите. Предприятия смогут воспользоваться усовершенствованиями, предназначенными для безопасности конфиденциальных данных, для эффективной защиты от вредоносных программ и обеспечения безопасного универсального доступа к корпоративным ресурсам и данным. Потребители могут пользоваться преимуществами компьютеров и Интернета, зная, что благодаря внедренным в Windows 7 современным технологиям безопасности конфиденциальность их личных данных находится под защитой. Кроме того, все пользователи оценят гибкие и доступные параметры конфигурации системы безопасности Windows 7, с помощью которых можно достичь баланса между безопасностью и удобством работы.

**Задание 1**

В операционной системе Windows 7 настроить политику учетных записей установив следующие параметры:

* максимальный срок действия пароля 45 дней;
* минимальная длина пароля 8 символов;
* минимальный срок действия пароля 5 дней;
* пароль должен отвечать требованиям сложности;
* пароли не должны повторяться;
* хранимые пароли должны быть зашифрованы.

**Задание 2**

В операционной системе Windows 7 настроить политику блокировки учетных записей установив следующие параметры:

* блокировка учетной записи на 60 минут после 5 попыток ввода неправильного пароля.
* сбор счетчика попыток через 30 минут.

# Лабораторная работа 2 Управление шаблонами безопасности в Windows 7

**Цель занятия**: Ознакомиться с возможностями операционной системы Windows 7 по управлению шаблонами безопасности. Изучить последовательность операций по управлению шаблонами безопасности операционной системы Windows 7. Приобрести практические навыки по защите компьютера под управлением операционной системы Windows 7.

**Норма времени**: 2 часа

**Методическое обеспечение:** методические указания к практической работе

**Теоретические сведения**

Управление шаблонами безопасности в Windows 7 осуществляется с помощью Редактора шаблонов безопасности, реализованного в виде оснастки ММС.

Он предназначен для создания и редактирования текстовых файлов конфигурации безопасности операционной системы Windows 7. Такие файлы значительно легче переносятся с одной системы на другую, чем соответствующие им базы данных безопасности.

Созданные при помощи оснастки Шаблоны безопасности текстовые файлы хранятся на жестком диске и, при необходимости, могут быть импортированы в базу данных безопасности. В этом случае все хранимые настройки безопасности начнут действовать.

Значения параметров обеспечения безопасности заносятся в текстовые файлы с расширением inf, называемые Шаблонами безопасности.

*Примечание. Новые Шаблоны безопасности не изменяют все старые настройки параметров системы безопасности, они лишь дополняют их, увеличивая (инкрементируя) степень защищенности компьютера.*

**Задание:**

Загрузить редактор Шаблона безопасности, редактировать шаблон безопасности и сохранить его с новым именем.

**Алгоритм выполнения работы.**

А). Загрузка оснастки Шаблоны безопасности.

Выберите кнопку Пуск в панели задач.

Перейдите к пункту Выполнить.

В открывшемся окне в поле ввода введите команду mmc.

В результате откроется консоль управления mmc.

В меню Консоль выберите команду Добавить или удалить оснастку (Рисунок 1) и нажмите кнопку Добавить.

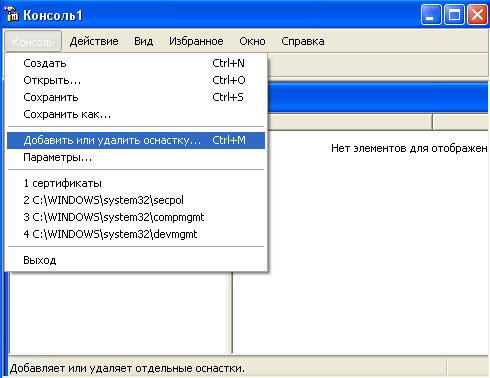


Рисунок 1

В поле Оснастка дважды щелкните Шаблоны безопасности.

Нажмите кнопку Закрыть.

В списке выбранных оснасток для новой консоли появится элемент Шаблоны безопасности.

Если на консоль не нужно добавлять другие оснастки, нажмите кнопку OK.

Чтобы сохранить эту консоль, в меню Консоль выберите команду Сохранить и укажите имя оснастки Шаблоны безопасности.

Закройте окно Консоли и выберите команду Пуск и далее Все программы.

Найдите пункт Администрирование и выберите подпункт Шаблоны безопасности (Теперь оснастка с Шаблоны безопасности доступна в меню Пуск).

Для просмотра значений имеющихся шаблонов в окне оснастки откройте, например, узел Шаблоны безопасности, щелчком выберите шаблон безопасности compatws (Рисунок 2) и просмотрите его папки Политика учетных записей, Локальная политика и др.

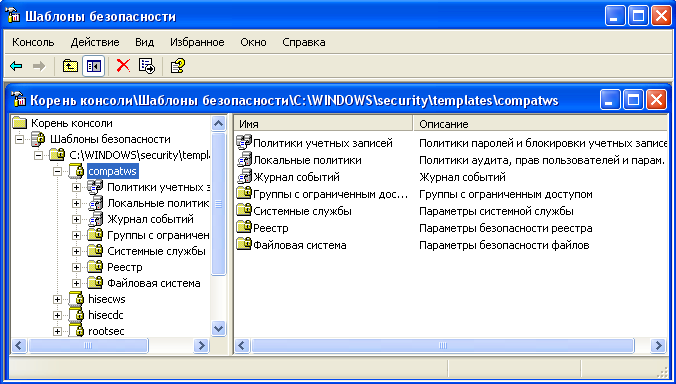


Рисунок 2

Помимо раскрытого шаблона безопасности compatws.inf существуют и другие стандартные шаблоны, конфигурации которых позволяют получить различные по надежности системы безопасности.

Б). Редактирование и сохранение шаблона безопасности.

Щелкните на одном из стандартных шаблонов безопасности (например, compatws), которые Вы видите в окне оснастки Шаблоны безопасности.

Если Вы хотите модифицировать какую-либо настройку безопасности, дважды щелкните на ней и отредактируйте значения параметров (Рисунок 3).

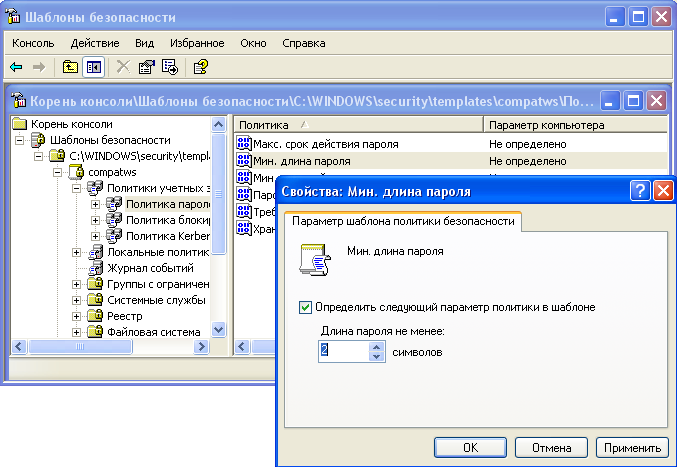


Рисунок 3

Для сохранения откорректированного стандартного шаблона безопасности под другим именем выполните следующие действия.

Укажите откорректированный стандартный шаблон (например, compatws), и нажмите правую кнопку мыши.

В появившемся контекстном меню выберите команду Сохранить как.

Введите с клавиатуры новое имя файла (например, custom). По умолчанию шаблоны безопасности располагаются в каталоге *%*SystemRoot%\Secunfy\Templates.

Пользовательский шаблон будет добавлен в определенную заранее конфигурацию безопасности и сохранен под введенным Вами именем.

Настроив Шаблон безопасности для одной ПЭВМ, Вы можете перенести его и на другие ПЭВМ Вашей рабочей группы. Шаблоны безопасности являются гибким и удобным инструментом по настройке системы безопасности операционной системы.

**Задания для самостоятельной работы**

Создайте на базе существующего Шаблона безопасности новый шаблон и дайте ему имя ПЗ-8. После этого зафиксируйте список шаблонов, скопировав изображение экрана в буфер для его отправки преподавателю в качестве отчета.

**Контрольные вопросы**

1. Для чего используются Шаблоны безопасности?
2. В каком месте на диске хранятся (по умолчанию) шаблоны безопасности?
3. Какие разделы включает стандартный Шаблон безопасности?

# Лабораторная работа 3 Разграничение полномочий и доступа к объектам операционной системы Unix

**Цель занятия**: Изучить политику безопасности операционной системы Windows 7

**Норма времени**: 2 часа

**Методическое обеспечение:** методические указания к практической работе

**Теоретические сведения**

 Разграничение доступа к объектам в операционных системах семейства Unix – файлам, каталогам, связям и специальным файлам (символьным или блочным устройствам ввода-вывода и именованным каналам) – осуществляется на базе хранящихся в индексе соответствующего объекта сведений о владельце объекта (UID) и его группе (GID), а также векторе доступа к объекту.

- Индекс файла – его управляющий блок, хранящийся в области индексов, отделенной от области файлов.

Структура каталога

Каталог – файл, состоящий из записей, соответствующих включенным в каталог файлам. Каждая запись состоит из номера индекса, связанного с данным файлом, и имени файла. Возможно создание множества файлов, связанных с одним и тем же индексом, ᴛ.ᴇ. с одной и той же областью внешней памяти (с помощью так называемых ссылок).

Вектор доступа

Представляет собой список контроля доступа фиксированной (а не произвольной, как в ОС Windows) длины. Первый элемент списка определяет права доступа к объекту его владельца, второй – членов его первичной группы, а третий – всех остальных пользователей системы. Суперпользователь root имеет полный доступ ко всем объектам в системе. Каждый элемент вектора доступа имеет длину 3 или 4 бита.

Виды доступа к объекту

- Возможны три вида доступа к объекту: чтение (r), запись (w) и выполнение (x). Для каталогов запись определяет создание, переименование и (или) удаление файлов, а выполнение – поиск файла в каталоге по заданному имени.

- Пример вектора доступа к файлу:

rwxr-xr--(или 0754 в восьмеричной форме)

(владелец файла вправе на полный доступ к нему, члены группы владельца – на чтение и выполнение файла, а все остальные пользователи – только на чтение файла).

*Надежность разграничения доступа к объектам в Unix*

Для того чтобы без использования системных команд изменить права доступа к объекту для конкретного пользователя, крайне важно иметь доступ к области индексов файловой системы, которые определены в специальном файле (к примеру, / dev / root). Но индекс этого файла также хранится в области индексов. По этой причине, в случае если не изменять права доступа ко всем системным объектам, которые заданы по умолчанию при установке операционной системы (что может сделать только суперпользователь), то можно гарантировать безопасность работы подсистемы разграничения доступа.

*Дополнительные биты в элементах управления доступом*

*В случае если* четвертый бит установлен в элементе вектора для владельца файла (SUID), то программный файл будет выполняться в сеансе любого пользователя с правами владельца этого файла. Это крайне важно , к примеру, при вызове команды passwd пользователем для изменения своего пароля. Обычный пользователь может иметь право смены своего пароля, но не может иметь право записи в файл паролей.

*В случае если* четвертый бит установлен в элементе вектора доступа для членов группы владельца (SGID), то данный программный файл будет выполняться в сеансе любого пользователя с правами членов группы владельца данного файла. В случае если SGID установлен в векторе доступа к каталогу, то все создаваемые пользователем файлы в данном каталоге будут иметь такой же идентификатор группы владельца, как и у каталога.

*В случае если* четвертый бит установлен в элементе вектора доступа для всех остальных пользователей (Sticky), то операционная система создает специальный текстовый образ программного файла. Чаще данный бит используется для каталогов и определяет запрет на удаление или переименование файлов других пользователей в данном каталоге. Это особенно важно для каталогов /tmp и /usr/tmp, чтобы одни пользователи не могли повредить работе других. Бит Sticky для каталогов должна быть установлен только администратором.

# Лабораторная работа 4 Настройка параметров аутентификации Windows 7

**Цель занятия**: Ознакомиться с основными параметрами механизма аутентификации операционной системы Windows 7. Изучить последовательность операций по настройке параметров аутентификации пользователей при входе в операционную систему. Приобрести практические навыки по защите компьютера от случайных или преднамеренных действий пользователей.

**Норма времени**: 2 часа

**Методическое обеспечение:** методические указания к практической работе

**Теоретические сведения**

В соответствии с сертификационными требованиями к системам безопасности операционных систем при подключении пользователей должен реализовываться механизм аутентификации и\или идентификации.

Идентификация и аутентификации применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

Идентификация - присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) - проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Настройка параметров аутентификации рассматриваемых операционных систем выполняется в рамках локальной политики безопасности.

Оснастка «Локальная политика безопасности» используется для изменения политики учетных записей и локальной политики на [локальном компьютере](ms-its:C:\WINDOWS\help\lpeconcepts.chm::/LPE_overview.htmHELP=glossary.hlp%20TOPIC=gls_local_computer).

При помощи оснастки «Локальная политика безопасности» можно определить:

кто имеет доступ к компьютеру;

какие ресурсы могут использовать пользователи на вашем компьютере;

включение и отключение записи действий пользователя или группы в журнале событий.

**Задание:**

Настроить параметры локальной политики безопасности операционной системы Windows 7.

**Алгоритм выполнения работы**

Для просмотра и изменения параметров аутентификации пользователей выполните следующие действия:

Выберите кнопку Пуск панели задач.

Откройте меню Настроить-Панель управления.

В открывшемся окне выберите ярлык Администрирование-Локальная политика безопасности.

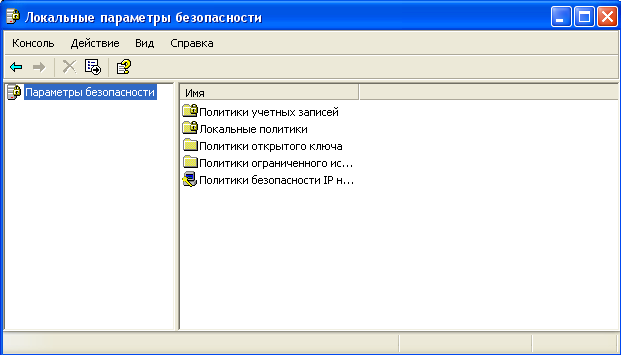


Рисунок 4

Выберите пункт Политика учетных записей (этот пункт включает два подпункта: Политика паролей и Политика блокировки учетной записи).

Откройте подпункт Политика паролей. В правом окне появится список настраиваемых параметров (Рисунок 5).

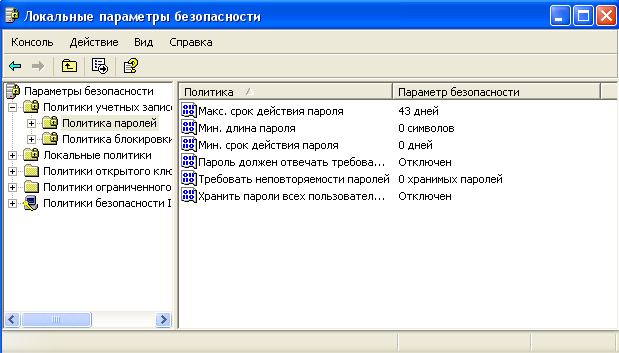


Рисунок 5

В показанном примере политика паролей соответствует исходному состоянию системы безопасности после установки операционной системы, при этом ни один из параметров не настроен. Значения параметров приведены в таблице 1.

Таблица 1

|  |  |
| --- | --- |
| Параметр | Значение |
| 1 | 2 |
| Требовать неповторяемости паролей. | Определяет число новых паролей, которые должны быть сопоставлены учетной записи пользователя, прежде чем можно будет снова использовать старый пароль. Это значение должно принадлежать диапазону от 0 до 24. |
| Максимальный срок действия пароля. | Определяет период времени (в днях), в течение которого можно использовать пароль, прежде чем система потребует от пользователя заменить его. Можно задать значение в диапазоне от 1 до 999 дней или снять всякие ограничения срока действия, установив число дней равным 0. |
| Минимальный срок действия пароля | Определяет период времени (в днях), в течение которого необходимо использовать пароль, прежде чем пользователь сможет заменить его. Можно задать значение в диапазоне от 1 до 999 дней или разрешить немедленное изменение, установив число дней равным 0. |
| Минимальная длина пароля. | Определяет наименьшее число символов, которые может содержать пароль учетной записи пользователя. Можно задать значение в диапазоне от 1 до 14 символов или отменить использование пароля, установив число символов равным 0. |
| Пароль должен отвечать требованиям сложности. | Определяет, должны ли пароли отвечать требованиям сложности.  Если эта политика включена, пароли должны удовлетворять следующим минимальным требованиям.  Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.  Пароль должен состоять не менее чем из шести символов.  В пароле должны присутствовать символы трех категорий из числа следующих четырех:  прописные буквы английского алфавита от A до Z;  строчные буквы английского алфавита от a до z;  десятичные цифры (от 0 до 9);  символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).  Проверка соблюдения этих требований выполняется при изменении или создании паролей. |
| Хранить пароли всех пользователей в домене, используя обратимое шифрование. | Определяет, следует ли в системах Windows 2000 Server, Windows 2000 Professional и Windows XP хранить пароли, используя обратимое шифрование. Эта политика обеспечивает поддержку приложений, использующих протоколы, которым для проверки подлинности нужно знать пароль пользователя. Хранить пароли, зашифрованные обратимыми методами, — это все равно, что хранить их открытым текстом. Поэтому данную политику следует использовать лишь в исключительных случаях, если потребности приложения оказываются важнее, чем защита пароля. |

Ознакомьтесь со свойствами всех параметров.

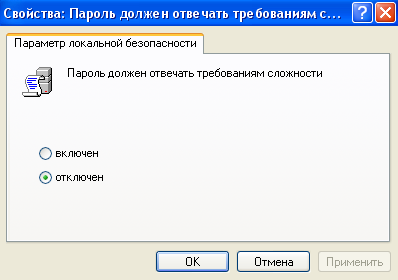
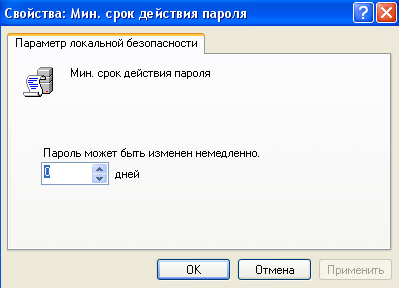


Рисунок 3

Для изменения требуемого параметра выделите его и вызовите его свойства из контекстного меню после нажатия правой кнопки мыши (или дважды щелкните на изменяемом параметре).

В результате этого действия появится одно из окон, показанных на рисунке 3.

Измените значение параметра и нажмите Ок.

Например, (обязательно выполнить и сохранить) выберите параметр Требовать неповторяемости паролей и измените его значение на 1.

Для настройки Политики блокировки учетной записи выберите этот подпункт и откройте его.

Значения параметров данного подпункта Политики учетных записей приведены в таблице 2.

Таблица 2

|  |  |
| --- | --- |
| Параметр | Значение |
| Пороговое значение блокировки | Определяет число неудачных попыток входа в систему, после которых учетная запись пользователя блокируется. Блокированную учетную запись нельзя использовать до тех пор, пока она не будет сброшена администратором или пока не истечет ее интервал блокировки. Можно задать значение в диапазоне от 1 до 999 или запретить блокировку данной учетной записи, установив значение 0. |
| Блокировка учетной записи на | Определяет число минут, в течение которых учетная запись остается блокированной, прежде чем будет автоматически разблокирована. Этот параметр может принимать значения от 1 до 99999 минут. Если установить значение 0, учетная запись будет блокирована на все время до тех пор, пока администратор не разблокирует ее явным образом.  Если пороговое значение блокировки определено, данный интервал блокировки должен быть больше или равен интервалу сброса. |
| Сброс счетчика блокировки через | Определяет число минут, которые должны пройти после неудачной попытки входа в систему, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99999 минут.  Если определено пороговое значение блокировки, данный интервал сброса не должен быть больше интервала [Блокировка учетной записи на](ms-its:spolsconcepts.chm::/508.htm). |

Ознакомьтесь со свойствами всех параметров.

Для изменения параметров воспользуйтесь алгоритмом, описанным в пунктах 8-10.

**Задания для самостоятельной работы**

Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» (Рисунок 3) и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения вашего задания и подлежит отправке преподавателю.

После успешного выполнения первого задания измените пароль Вашей учетной записи, а в качестве нового пароле укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности. Результаты анализа представить преподавателю.

Проведите эксперименты с другими параметрами Политики учетных записей.

**Контрольные вопросы**

1. Что такое аутентификация и идентификация?
2. Для чего применяются эти механизмы?
3. Что можно настроить с помощью оснастки Локальная политика безопасности.

**Описание формы отчета**

Выполненное задание для самостоятельной работы и ответы на контрольные вопросы необходимо выслать для проверки преподавателю.

# Лабораторная работа 5 Назначение прав пользователей при произвольном управлении доступом в Windows 7

**Цель занятия**: Ознакомиться с возможностями системы безопасности операционной системы Windows 7 по назначению прав доступа пользователей. Изучить последовательность операций по созданию новых пользователей и групп, а также назначению их прав доступа. Приобрести практические навыки по управлению правами доступа в операционной системе Windows 7.

**Норма времени**: 2 часа

**Методическое обеспечение:** методические указания к практической работе

**Теоретические сведения**

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.

Обычно полномочия субъекта представляются списком ресурсов, доступным пользователю и правами по доступу к каждому ресурсу из списка.

При разграничении доступа по спискам задаются соответствия: каждому пользователю — список ресурсов и прав доступа к ним или каждому ресурсу — список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Задание:

Создать учетную запись и локальную группу, изменить принадлежность пользователя к локальной группе и блокировать учетную запись пользователя.

**Алгоритм выполнения работы.**

А) Создание учетной записи.

Откройте оснастку Управление компьютером в разделе Администрирование Панели управления (Рисунок 1).

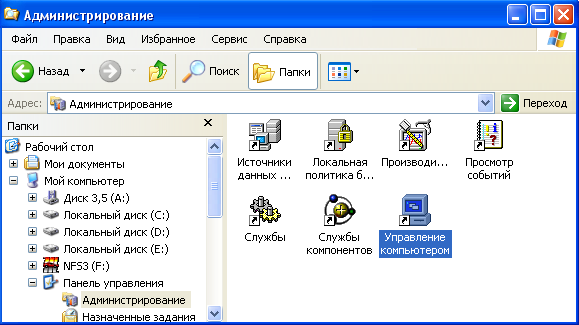


Рисунок 1

В оснастке Локальные пользователи и группы установите указатель мыши на папку Пользователи и нажмите правую кнопку.

В появившемся контекстном меню выберите команду Новый пользователь (Рисунок 2). Появится окно диалога Новый пользователь (Рисунок 3).

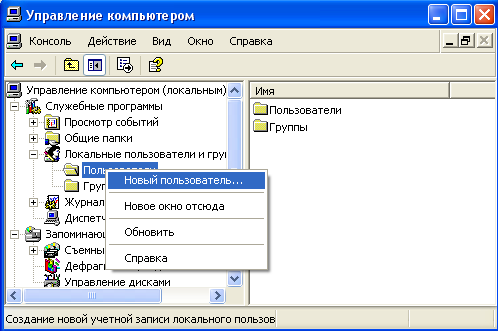


Рисунок 2

В поле Пользователь введите имя создаваемого пользователя, например, свою фамилию.

Примечание. Имя пользователя должно быть уникальным для компьютера. Оно может содержать до 20 символов верхнего и нижнего регистра. Ниже приведены символы, применение которых в имени пользователя недопустимо:"/ \ []:; =,+\*?<>

Имя пользователя не может состоять целиком из точек и пробелов.

В поле Полное имя введите полное имя создаваемого пользователя.

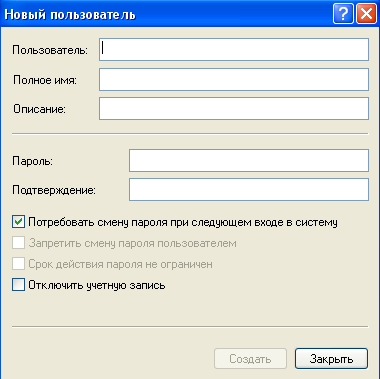


Рисунок 3

В поле Описание введите описание создаваемого пользователя или его учетной записи, например, "*студент ……….*".

В поле Пароль введите пароль пользователя и в поле Подтверждение подтвердите его правильность вторичным вводом.

Примечание. Длина пароля не может превышать 14 символов*.*

Установите или снимите флажки:

* потребовать смену пароля при следующем входе в систему;
* запретить смену пароля пользователем;
* срок действия пароля не ограничен;
* отключить учетную запись.

Чтобы создать еще одного пользователя, нажмите кнопку Создать и повторите шаги с 1 по 8. Для завершения работы нажмите кнопку Создать и затем Закрыть.

Б) Создание локальной группы.

В окне оснастки Локальные пользователи и группы установите указатель мыши на папке Группы и нажмите правую кнопку.

В появившемся контекстном меню выберите команду Новая группа.

В поле Имя группы (Рисунок 4) введите имя новой группы, например, Студенты.

Примечание. Имя локальной группы должно быть уникальным в пределах компьютера. Оно может содержать до 256 символов в верхнем и нижнем регистрах.

В поле Описание введите описание новой группы.

В поле Члены группы можно сразу же добавить пользователей и группы, которые войдут в данную группу: для этого нужно нажать кнопку Добавить и выбрать их в списке.

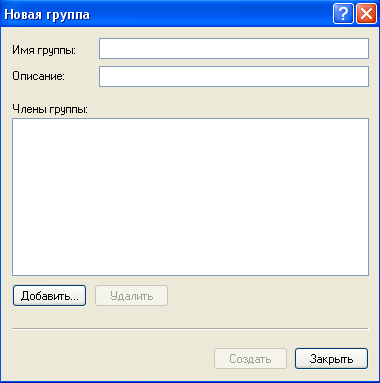


Рисунок 4

Для завершения нажмите кнопку Создать и затем Закрыть.

Для изменения членства в локальной группе выполните следующие действия.

В окне оснастки Локальные пользователи и группы щелкните на папке Группы.

В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку.

В появившемся контекстном меню выберите команду Добавить в группу или Свойства.

Для того, чтобы добавить новые учетные записи в группу, нажмите кнопку Добавить (Рисунок 5).

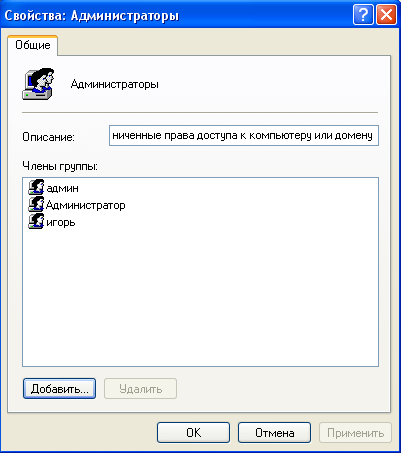


Рисунок 5

Далее следуйте указаниям окна диалога Выбор: Пользователи или Группы.

Для того, чтобы удалить из группы некоторых пользователей, в поле Члены группы (Рисунок 5) окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку Удалить.

Примечание В локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и глобальные группы, созданные в домене, к которому принадлежит компьютер или в доверяемых доменах. Встроенные группы не могут быть удалены. Удаленные группы не могут быть восстановлены. Удаление группы не отражается на входящих в нее пользователей.

В) Временная блокировка учетной записи.

Откройте оснастку Управление компьютером.

Для этого либо выберите на Рабочем столе ярлык Мой компьютер и нажмите правую клавишу Мыши, после чего выберите пункт контекстного меню Управление, либо воспользуйтесь разделом Администрирование в Панели управления.

В открывшейся оснастке выберите пункты Служебные программы/Локальные пользователи и группы (Рисунок 2).

Откройте папку Пользователи и выберите учетную запись Гость.

Нажмите правую клавишу мыши и выберите пункт Свойства.

В открывшемся окне снимите отметку пункта Отключить учетную запись (Рисунок 6).

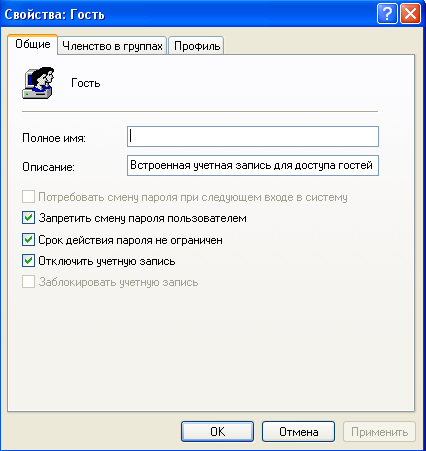


Рисунок 6

Нажмите кнопку ОК и сделайте вывод о состоянии учетной записи.

Выполните пункт 5 и отметьте пункт Отключить учетную запись.

**Задания для самостоятельной работы**

Создайте учетную запись ПЗ-7, используя команду Print Screen клавиатуры, сохраните копию экрана со списком пользователей Вашего компьютера (для этого, после нажатия клавиши Print Screen вставьте скопированное изображение в новый документ Word) для представления в качестве отчета преподавателю.

Создайте группу Информационная безопасность и, как в первом задании, сохраните окно со списком групп Вашего компьютера для представления преподавателю.

Заблокируйте учетную запись ПЗ-7 и после этого удалите.

**Контрольные вопросы**

1. Какие методы управления доступом Вам известны?
2. Чем отличается мандатное управление доступом от дискретного?
3. Допустимо ли имя пользователя ПЗ8\44? Почему?

# Лабораторная работа 6 Настройка параметров регистрации и аудита в Windows 7

**Цель занятия**: Ознакомиться с возможностями операционной системы Windows 7 по регистрации и аудиту событий системы безопасности. Изучить последовательность операций по настройке параметров регистрации и аудита системы безопасности. Приобрести практические навыки по анализу событий системы безопасности операционной системы Windows 7.

**Норма времени**: 2 часа

**Методическое обеспечение:** методические указания к практической работе

**Теоретические сведения**

Регистрация является еще одним механизмом обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения безопасности, фиксирующий все события, касающиеся безопасности. Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей и т.д.

Аудит – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Практическими средствами регистрации и аудита являются:

* различные системные утилиты и прикладные программы;
* регистрационный (системный или контрольный) журнал.

Первое средство является обычно дополнением к мониторингу, осуществляемому администратором системы. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

Регистрационный журнал — это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

**Задание:**

Активизировать механизмы регистрации и аудита операционной системы Windows 7 и настройка параметров просмотра аудита папок и файлов

**Алгоритм выполнения работы.**

А) Активизация механизма регистрации и аудита с помощью оснастки Локальные политики безопасности.

Для активизации аудита на изолированном компьютере выполните следующие действия.

1. Выберите кнопку Пуск панели задач.

2. Откройте меню Настроить/Панель управления.

3. В открывшемся окне выберите ярлык Администрирование/Локальная политика безопасности.

4 .Выберите пункт Политика аудита (Рисунок 1).

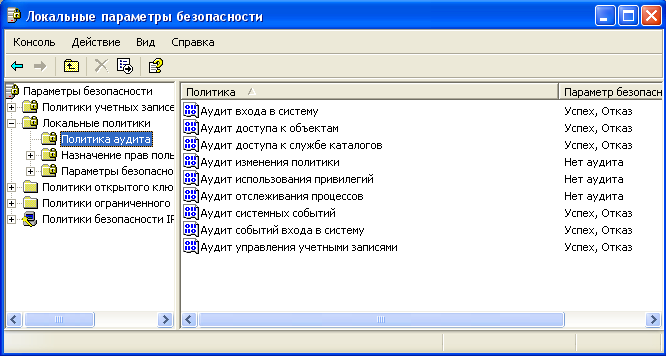


Рисунок 1

5. Для включения или отключения параметров аудита выберите требуемый параметр и дважды щелкните левой клавишей мыши.

6. Для каждого параметра можно задать аудит успехов или отказов, либо вообще отключить аудит событий данного типа (Рисунок 2).

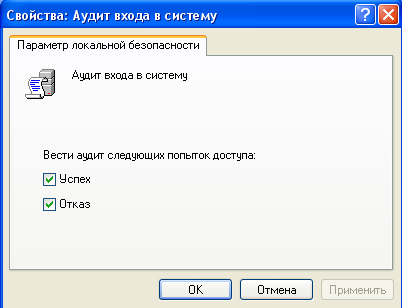


Рисунок 2

7. Значения параметров политики аудита приведены в таблице 1.

Таблица 1

|  |  |
| --- | --- |
| Параметр | Значение |
| 1 | 2 |
| Аудит событий входа в систему | Определяет, подлежит ли аудиту каждая попытка пользователя войти в систему или выйти из нее на другом компьютере, при условии, что данный компьютер используется для проверки подлинности учетной записи.  Если этот параметр политики определен, можно задать аудит успехов или отказов, либо вообще отключить аудит событий данного типа. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему. |
| Аудит управления учетными записями | Определяет, подлежат ли аудиту все события, связанные с управлением учетными записями на компьютере. К таким событиям относятся следующие события:  создание, изменение или удаление учетной записи пользователя или группы;  переименование, отключение или включение учетной записи пользователя;  задание или изменение пароля. |
| Аудит доступа к службе каталогов | Определяет, подлежит ли аудиту событие доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом. |
| Аудит входа в систему | Определяет, подлежит ли аудиту каждая попытка пользователя войти в систему или выйти из нее на данном компьютере, или подключиться к нему через сеть. |
| Аудит доступа к объектам | Определяет, подлежит ли аудиту событие доступа пользователя к объекту — например, к файлу, папке, разделу реестра, принтеру и т.п., — для которого задана собственная системная таблица управления доступом. |
| 1 | 2 |
| Аудит изменения политики | Определяет, подлежит ли аудиту каждый факт изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений. |
| Аудит использования привилегий | Определяет, подлежит ли аудиту каждая попытка пользователя воспользоваться предоставленным ему правом. |
| Аудит отслеживания процессов | Определяет, подлежат ли аудиту такие события, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту. |
| Аудит системных событий | Определяет, подлежат ли аудиту события перезагрузки или отключения компьютера, а также события, влияющие на системную безопасность или на журнал безопасности. |

По умолчанию все параметры политики аудита выключены.

Включите аудит успеха и отказа для всех параметров.

Для этого выполните пункт 5.

Нажмите кнопку ОК.

Б) Настройка и просмотр аудита папок и файлов (Доступно только на томах NTFS).

Чтобы настроить, просмотреть или изменить настройки аудита файлов и папок выполните следующие действия.

Установите указатель мыши на файл или папку, для которой следует выполнить аудит и нажмите правую кнопку.

В появившемся контекстном меню выберите команду Свойства.

В окне свойств папки или файла перейдите на вкладку Безопасность.

На вкладке Безопасность нажмите кнопку Дополнительно и затем перейдите на вкладку Аудит.

Если вы хотите настроить аудит для нового пользователя или группы на вкладке Аудит нажмите кнопку Добавить.

Появится диалоговое окно Выбор: Пользователь, Компьютер или Группа.

Выберите имя нужного пользователя или группы и нажмите кнопку ОК. Откроется окно диалога Элемент аудита для. Здесь вы сможете ввести все необходимые параметры аудита.

В списке Применять укажите, где следует выполнять аудит (это поле ввода доступно только для папок).

В группе Доступ следует указать, какие события следует отслеживать: окончившиеся успешно (Успех), неудачно (Отказ) или оба типа событий.

Применять этот аудит к объектам и контейнерам только внутри этого контейнера определяет, распространяются ли введенные Вами настройки аудита на файлы и папки, находящиеся ниже по дереву каталогов файловой системы (флажок не установлен). В обратном случае, установите флажок (или выберите в списке Применять опцию Только для этой папки. Это позволит не выполнять аудит для тех объектов файловой системы, которые не представляют интереса.

После завершения настройки аудита для папки или файла нажмите несколько раз кнопку ОК, чтобы закрыть все окна диалога.

Если вы хотите просмотреть или изменить настройки аудита для уже существующего пользователя или группы, нажмите кнопку Показать/Изменить. Появится окно диалога Элемент аудита для. Здесь Вы сможете выполнить все необходимые изменения параметров аудита для выбранного Вами пользователя или группы. По окончании внесения изменений нажмите кнопку ОК.

Примечание. После включения аудита операционная система Windows 7 начинает отслеживать события, связанные с безопасностью. Полученную в результате информацию можно просмотреть с помощью оснастки Просмотр событий. При *просмотре журнала событий можно выяснить, кто предпринял попытку выполнения неразрешенного ему действия.*

*Для того чтобы иметь возможность настраивать аудит для файлов и папок, необходимо иметь права администратора.*

Б) Просмотр событий в журнале событий.

Для просмотра событий выполните следующие действия.

Выберите кнопку Пуск панели задач.

Откройте меню Настроить/Панель управления.

В открывшемся окне выберите ярлык Администрирование и далее Просмотр событий.

В открывшемся окне выберите пункт Безопасность (Рисунок 3).

В правой половине открытого окна появится список всех зарегистрированных событий.

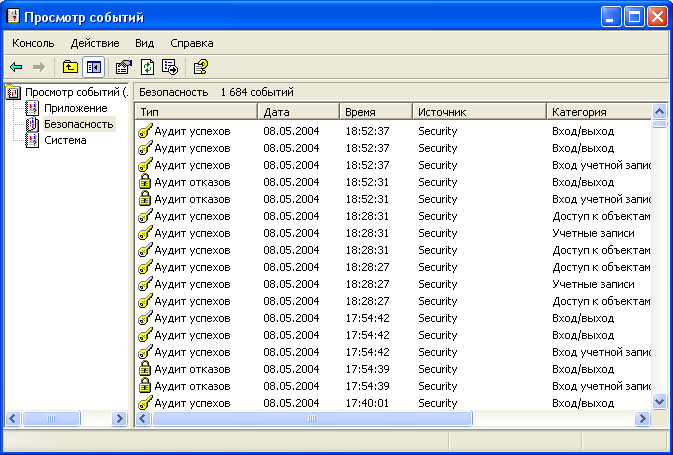


Рисунок 3

Для просмотра требуемого события вызовите его свойства из контекстного меню или дважды щелкните по его названию левой клавишей мыши.

В результате появится окно, как показано на рисунке 4.

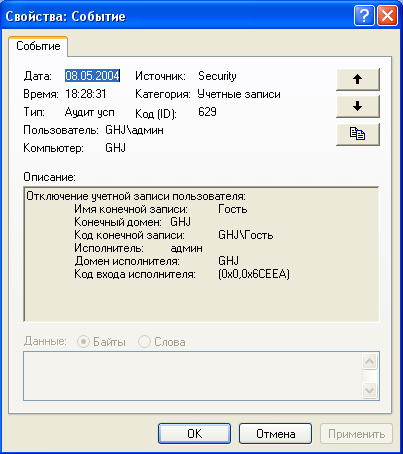


Рисунок 4

В показанном примере зафиксирован успех отключения учетной записи Гость пользователем Админ 8.05.04 в 18.28.31.

В примере, показанном на рисунке 5, зафиксирован отказ входа всистему пользователюNT AUTHORITY\SYSTEM(системная учетная запись)08.05.04 в 17:39:58по причине«неизвестное имя пользователя или неверный пароль».

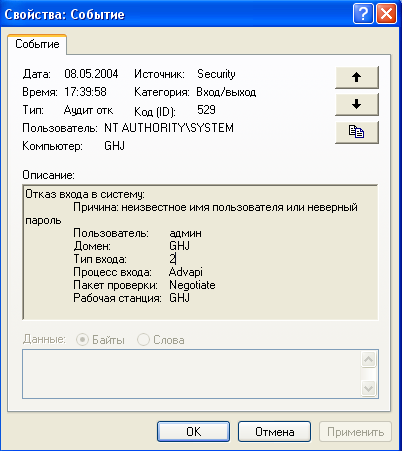


Рисунок 5

Таким образом, просмотр журнала событий позволяет в полной мере проанализировать действия пользователей и процессов.

**Задания для самостоятельной работы**

Включите аудит успеха и отказа всех параметров (используйте задание А).

Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем. Откройте журнал событий, найдите соответствующую запись и скопируйте экран в буфер (Print Screen) для его представления преподавателю.

Удалите созданную ранее учетную запись ПЗ-7 и зафиксируйте все события системного журнала, связанные с этим действием для представления преподавателю отчета.

**Контрольные вопросы**

* Чем отличаются регистрация и аудит?
* Что является средствами регистрации и аудита?
* Какие события фиксируются в системном журнале?
* Что фиксирует система при регистрации событий?

# Практическая работа 1 Методы криптографического преобразования данных

**Цель занятия**: Ознакомиться с возможностями операционной системы Windows 7 по регистрации и аудиту событий системы безопасности. Изучить последовательность операций по настройке параметров регистрации и аудита системы безопасности. Приобрести практические навыки по анализу событий системы безопасности операционной системы Windows 7.

**Норма времени**: 2 часа

**Методическое обеспечение:** методические указания к практической работе

**Теоретические сведения**

Проблемой защиты информации путем ее преобразования занимается криптология (kryptos – тайный, logos – наука). Криптография занимается поиском и исследованием математических методов преобразования информации. Перечислим основные понятия:

Алфавит – конечное множество используемых для кодирования информации знаков.

Текст – упорядоченный набор из элементов алфавита.

Шифрование – преобразовательный процесс

Дешифрование – обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования исходных текстов.

Существует много различных методов шифрования. Рассмотрим некоторые из них.

Методы перестановки.

Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые разновидности этого метода.

Самая простая перестановка – написать исходный текст задом на перед и одновременно разбить шифрограмму на пятерки букв. Например из фразы

ПУСТЬ БУДЕТ ТАК КАК МЫ ХОТЕЛИ

получим сделаем шифротекст:

в исходной фразе до кратности пяти не хватает одной буквы. Допишем в конец любую букву и перевернем фразу:

ПУСТЬ БУДЕТ ТАК КАК МЫ ХОТЕЛИО

ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЬТСУП

Во время Гражданской войны в США в ходу был следующий шифр: исходную фразу писали в несколько строк (например 15). Оставшиеся пустыми ячейки таблицы заполняли «пустышками» (любыми символами).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| П | У | С | Т | Ь | Б | У | Д | Е | Т | Т | А | К | К | А |
| К | М | Ы | Х | О | Т | Е | Л | И | К | Л | М | Н | О | П |

После этого вертикальные столбцы по порядку писали в строку с разбивкой на пятерки:

ПКУМС ЫТХЬО БТУЕД ЛЕИТК ТЛАМК НКОАП

Вариант этого шифра: исходную фразу писать в столбцы, а затем на пятерки разбивать строки:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| П | С | Ь | У | Е | Т | К | А | М | Х | Т | Л | А | В | Д |
| У | Т | Б | Д | Т | А | К | К | Ы | О | Е | И | Б | Г | Е |

ПСЬУЕ ТКАМХ ТЛАВД УТБДТ АККЫО ЕИБГЕ

Исходный текст можно записать в квадратную  таблицу и списать из нее, например по диагоналям:



ПУУСДК ТЕКХЬТ АОАБТК ТБЖАМЕ ВЗЫЛГИ ИДКЕЛМ

Часто используются перестановки с ключом

Выберем в качестве ключа слово «информация». Пронумеруем ключ (первая, из имеющихся в ключе, в алфавите буква А, следовательно ей присваивается номер 1; следующая по алфавиту буква И, следовательно первая буква И будет иметь номер 2, а вторая – 3; далее идет буква М, ей присваиваем номер 4 и т.д.):

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| и | н | ф | о | р | м | а | ц | и | я |
| 2 | 5 | 8 | 6 | 7 | 4 | 1 | 9 | 3 | 10 |

Запишем в таблицу нашу фразу под ключом. Оставшиеся ячейки до конца строки заполняют «пустышками».

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| и | н | ф | о | р | м | а | ц | и | я |
| 2 | 5 | 8 | 6 | 7 | 4 | 1 | 9 | 3 | 10 |
| П | У | С | Т | Ь |  | Б | У | Д | Е |
| Т |  | Т | А | К |  | К | А | К |  |
| М | Ы |  | Х | О | Т | Е | Л | И | Ф |

Переписываем столбцы, учитывая их номер:

БКЕПТМДКИ  ТУ ЫТАХЬКОСТ УАЛЕ Ф

Для дешифрования зашифрованный текст записывается в таблицу по столбцам, учитывая их номер.

 Гамильтоновы пути.

Выбираем ключ и нумеруем его как в предыдущем  методе. Символы шифруемой фразы нумеруем по порядку в пределах ключа. Затем переставляем символы исходного текста, учитывая номер ключа.

Ключ:л е г е н д а

         6 4 2 5 7 3 1

[](http://eva-npk.ucoz.ru/_pu/0/99264050.png)

 Получаем текст:http://eva-npk.ucoz.ru/_pu/0/84854946.png

**Шифрование методом гаммирования.**

Суть этого метода состоит в том, что символы исходного текста последовательно складываются с символами некоторой специальной последовательности (гаммы).

Символы исходного текста и гаммы заменяются их числовыми эквивалентами по номеру в алфавите. Обозначим символы исходного текста хi, символы гаммы – gi, число символов в алфавите – n, зашифрованный текст – yi.

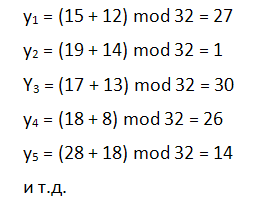
Тогда шифрование выполняется по формуле http://eva-npk.ucoz.ru/_pu/0/16827265.png

Дешифрование будет выполняться по формуле http://eva-npk.ucoz.ru/_pu/0/07641705.png.

Например.

Запишем исходную фразу, а над ней гамму. В качестве гаммы возьмем слово монитор. Все символы заменяем числовыми эквивалентами.

[](http://eva-npk.ucoz.ru/_pu/0/78480394.png)



**Задание**

1. Зашифруйте полученную у преподавателя фразу всеми методами перестановки.
2. Зашифруйте фразу методом гаммирования..
3. Расшифруйте полученную у преподавателя информацию
4. Оформите отчёт.

# Лабораторная работа 7 Использование функций криптографического интерфейса (CryptoAPI) операционной системы Windows для защиты информации.

**Цель занятия**: изучить принципы построения и использования CryptoAPI. Ознакомиться с базовыми криптографическими функциями. На практике усвоить принципы организации программ, обеспечивающих создание и управления ключами шифрования.

**Норма времени**: 2 часа

**Методическое обеспечение:** методические указания к практической работе

Теоретические сведения

Принципы построения и использования криптографического интерфейса Windows (CryptoAPI)

Криптографический интерфейс приложений операционной сис­темы Windows представляет собой набор констант, типов данных и функций, предназначенных для выполнения операций шифрова­ния, расшифрования, получения и проверки ЭЦП, генерации, хра­нения и распределения ключей шифрования. Эти услуги для при­ложений предоставляют провайдеры криптографического обслужи­вания (Cryptographic Service Provider, CSP) - динамически компо­нуемые библиотеки (DLL), экспортирующие единый набор объек­тов, определяемый интерфейсом CryptoAPI.

Взаимодействие между приложением и CSP строится на основе следующих принципов:

приложение не имеет прямого доступа к изготовлению и хра­нению ключей шифрования (нет риска их потери из-за ошибок в приложении);

приложение не определяет деталей выполнения криптогра­фических операций, а лишь указывает на требуемые от CSP дейст­вия (например, зашифровать по заданному алгоритму данные и получить для них ЭЦП);

приложение не обрабатывает данных, по которым проводится аутентификация пользователя, а предоставляет это CSP, который имеет лучшие возможности для проверки подлинности пользователя (например, может использовать аутентификацию на основе биомет­рических признаков или ключевой информации, размещенной на смарт-картах или других элементах аппаратного обеспечения); в этом случае из-за ошибок в приложении не может произойти утечка конфи­денциальной информации о пользователе (например, его пароле).

На рис. 1 приведена архитектура криптографической подсис­темы Windows. Вызовы функций CryptoAPI обрабатываются моду­лем операционной системы advapi32.dll, который преобразует их в вызовы функций интерфейса провайдера криптографического об­служивания (Cryptographic Service Provider Interface, CryptoSPI). Для обеспечения аутентичности и подлинности CSP он снабжается ЭЦП, которая периодически проверяется операционной системой в ходе сеанса работы пользователя. Получение ЭЦП производится корпорацией Microsoft на основе хеш-значения CSP, представлен­ного изготовителем этой библиотеки.

Каждый CSP характеризуется своим присвоенным производи­телем именем (строкой символов) и типом (целым числом от 1 до 999), определяющим поддерживаемые этим провайдером криптографические алгоритмы

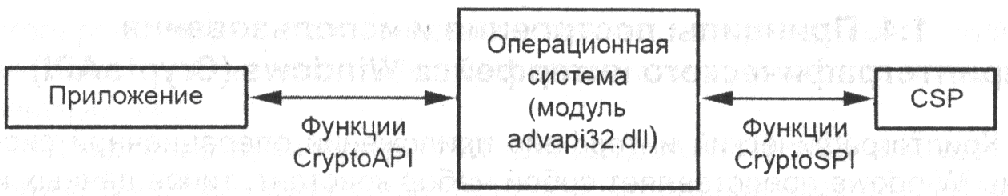


Рис. 1. Взаимодействие приложения и криптопровайдера

В табл. 1 приведены некоторые предо­пределенные типы криптопровайдеров.

*Основные атрибуты CSP*

* К основным атрибутам CSP относятся:
* реализованный (обязательно) алгоритм ЭЦП (всегда единст­венный);
* реализованная (обязательно) функция хеширования;
* длина ключей асимметричного шифрования;
* формат ЭЦП;
* форматы блоков, в которых открытый и (возможно) секретный ключи асимметричного шифрования экспортируются из CSP;
* реализованный (возможно) алгоритм обмена сеансовыми ключами симметричного шифрования (всегда единственный);
* реализованные (возможно) алгоритмы симметричного шифро­вания (конкретный CSP может поддерживать часть таких алгоритмов, определенных для соответствующего типа криптопровайдера);
* алгоритм генерации сеансового ключа из хеш-значения;
* длины сеансовых ключей (в зависимости от алгоритма);
* формат блока сеансового ключа при его экспорте из CSP;

Таблица 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Символическая константа типа (ее численное значение)* | *Алгоритм обмена се­ансовыми ключами* | *Алго­ритм ЭЦП* | *Алгоритмы симметрич­ного шифро­вания* | *Функ­ции хеши­рова­ния* |
| PROV\_RSA\_FULL (1) | RSA | RSA | RC2, RC4, DES, 3-DES | MD2, MD4, MD5, SHA |
| PROV\_RSA\_SIG (2) |  | RSA |  | MD5, SHA |
| PROV\_DSS (3) |  | DSS |  | SHA |
| PROV\_FORTEZZA (4) | DH | DSS | Skipjack | SHA |
| PROV\_MS\_EXCHANGE (5) | RSA | RSA | CAST, RC2, DES, 3-DES | MD5 |
| PROV\_SSL (6) | RSA | RSA | Разные | Разные |
| PROV\_RSA\_SCHANNEL (12) | RSA | RSA | RC2, RC4, DES, 3-DES | MD5, SHA |
| PROV\_DSS\_DH (13) | DH | DSS | CYLINK MEK, RC2, RC4, DES, 3-DES | MD5, SHA |
| PROV\_EC\_ECDSA\_SIG (14) |  | ЕС |  | SHA |
| PROV\_DH\_SCHANNEL (18) | DH | DSS | CYLINK MEK, RC2, RC4, DES, 3-DES | MD5, SHA |
| PROV\_RSA\_AES (24) | RSA | RSA | RC2, RC4, DES, 3-DES, AES | MD2, MD4, MD5, SHA |

Информация об установленных на компьютере криптопровай-дерах содержится в реестре Windows в разделе HKEY\_LOCAL\_MACHINE \ Software \ Microsoft \ Cryptography \ De­faults. В подразделе Provider размещается информация о пути к библиотеке, ЭЦП и типе каждого CSP (по его имени), а в подразде­ле Provider Types - сведения о полных именах криптопровайдера и его типа.

*Контейнеры ключей*

Для каждого зарегистрированного у него пользователя или кон­кретного приложения CSP хранит контейнер ключей асимметрично­го шифрования (key set), который может включать в себя две пары ключей - открытый и секретный ключи для обмена сеансовыми ключами, а также открытый и секретный ключи для ЭЦП. Ключи симметричного шифрования (сеансовые ключи) не сохраняются CSP и об их сохранении (или правильной повторной генерации) должно позаботиться приложение.

Контейнер ключей может храниться криптопровайдером в реест­ре Windows, в файле на диске или на защищенном от несанкциони­рованного чтения съемном носителе (смарт-карте, USB-ключе и т.п.).

*Криптопровайдеры от Microsoft*

Вместе с операционной системой Windows корпорация Microsoft поставляет несколько встроенных криптопровайдеров типа PROV\_RSA\_FULL:

*Microsoft Base Cryptographic Provider v1.0* - поддерживает алго­ритмы симметричного шифрования RC2 и RC4 с длиной ключа от 40 (по умолчанию) до 64 бит, DES, алгоритм ЭЦП с длиной ключа от 384 до 16384 бит (по умолчанию 512), алгоритм обмена сеансовыми ключами с длиной ключа от 384 до 1024 бит (по умолчанию 512);

*Microsoft Enhanced Cryptographic Provider v1.0* - поддерживает алгоритмы симметричного шифрования RC2 и RC4 с длиной ключа от 40 до 128 (по умолчанию) бит, DES, 3-DES, 3-DES Two Key, ал­горитмы ЭЦП и обмена сеансовыми ключами с длиной ключа от 384 до 16384 бит (по умолчанию 1024);

*Microsoft Strong Cryptographic Provider* - поддерживает алгорит­мы симметричного шифрования RC2 и RC4 с длиной ключа от 40 (по умолчанию в Windows 2000) до 128 (по умолчанию в Windows МЕ/ХР) бит, DES, 3-DES, 3-DES Two Key, алгоритмы ЭЦП и обмена сеансовыми ключами с длиной ключа от 384 до 16384 бит (по умолчанию 512 в Windows 2000 и 1024 в Windows МЕ/ХР).

Первый из указанных выше криптопровайдеров является криптопровайдером по умолчанию. Все эти криптопровайдеры хранят контейнеры ключей пользователей в реестре Windows.

С операционными системами Windowsтакже поставляется еще ряд криптопровайдеров**:**

*Microsoft Exchange Cryptographic Provider v1.0* (типа PROV\_MS\_EXCHANGE) – поддерживает алгоритмы симметричного шифрования RC2 и RC4 с длиной ключа от 40 до 128 (по умолча­нию) бит, DES, 3-DES, 3-DES Two Key, алгоритм ЭЦП с длиной ключа 512 бит, алгоритм обмена сеансовыми ключами с длиной ключа 512 бит;

*Microsoft Base DSS Cryptographie Provider* (типа PROV\_DSS) -поддерживает алгоритмы ЭЦП и обмена сеансовыми ключами с длиной ключа от 512 до 1024 (по умолчанию) бит;

*Microsoft Base DSS and Diffie-Hellman Cryptographie Provider* (ти­па PROV\_DSS\_DH) - поддерживает алгоритмы симметричного шифрования CYLINK МЕК с длиной ключа 40 бит, RC2 и RC4 с длиной ключа от 40 (по умолчанию) до 56 бит, DES, алгоритм ЭЦП с длиной ключа от 512 до 1024 (по умолчанию) бит, алгоритм обме­на сеансовыми ключами с длиной ключа от 512 (по умолчанию) до 1024 бит;

*Microsoft Enhanced DSS and Diffie-Hellman Cryptographie Provider* (типа PROV\_DSS\_DH) - поддерживает алгоритмы симметричного шифрования CYLINK МЕК с длиной ключа 40 бит, RC2 и RC4 с длиной ключа от 40 (по умолчанию в Windows ME и 2000) до 128 (по умолчанию в Windows ХР) бит, DES, 3-DES, 3-DES Two Key, алгоритм ЭЦП с длиной ключа от 512 до 1024 (по умолчанию) бит, алгоритм обмена сеансовыми ключами с длиной ключа от 512 (по умолчанию в Windows ME и 2000) до 4096 бит (в Windows ХР длина ключа обмена по умолчанию 1024 бит).

Вместе с операционными системами Windows 2000/ХР допол­нительно поставляются криптопровайдеры:

*Microsoft DH SChannel Cryptographie Provider* (типа PROV\_DH\_SCHANNEL) - поддерживает алгоритмы симметричного шифрования CYLINK МЕК с длиной ключа 40 бит, RC2 и RC4 с дли­ной ключа от 40 (по умолчанию) до 128 бит, DES, 3-DES, 3-DES Two Key, алгоритм ЭЦП с длиной ключа от 512 до 1024 (по умолчанию) бит (в Windows 2000 только 1024 бит), алгоритм обмена сеансовыми ключами с длиной ключа от 512 (по умолчанию) до 4096 бит;

*Microsoft RSA SChannel Cryptographie Provider* (типа PROV\_RSA\_SCHANNEL) - поддерживает алгоритмы симметрично­го шифрования RC2 и RC4 с длиной ключа от 40 до 128 (по умол­чанию) бит, DES, 3-DES, 3-DES Two Key, алгоритмы ЭЦП и обмена сеансовыми ключами с длиной ключа от 384 до 16384 бит (по умолчанию 1024 бита);

*Microsoft Enhanced RSA and AES Cryptographie Provider (Proto­type)* (типа PROV\_RSA\_AES) - поддерживает алгоритмы симмет­ричного шифрования RC2 и RC4 с длиной ключа от 40 до 128 (по умолчанию) бит, DES, 3-DES, 3-DES Two Key, AES (с длиной ключа128, 192 и 256 бит), алгоритмы ЭЦП и обмена сеансовыми ключами с длиной ключа от 384 до 16384 бит (по умолчанию 1024 бит).

*Версии CryptoAPI*

Существуют две версии CryptoAPI: 1.0 и 2.0. В CryptoAPI 1.0 поддерживаются базовые функции для выполнения всех основных криптографических операций. В CryptoAPI 2.0 (библиотека crypt32.dll) введены дополнительные функции для поддержки ин­фраструктуры открытых ключей.

Для доступа к криптографическим функциям из программ и сце­нариев на языках Visual Basic, VBScript, JavaScript и аналогичных им в операционной системе Windows предназначен набор много­компонентных объектов CAPICOM (CryptoAPI Component Object Model, библиотека capicom.dll).

*Обзор функций СгурtоАРI 1.0*

Основные функции CryptoAPI 1.0 приведены в табл. 2.

Таблица 2.

|  |  |
| --- | --- |
| *Название функции* | *Краткое описание функции* |
| CryptEncrypt CryptDecrypt | Симметричное шифрова­ние и расшифрование дан­ных |
| CryptCreateHash CryptDestroyHash | Создание пустого хеш-значения и освобождение его дескриптора |
| CryptHashData CryptHashSessionKey | Хеширование(добавление к хеш-значению) произ­вольных данных и сеансо­вого ключа |
| CryptGetHashParam CryptSelHashParam | Получение и установка па­раметров хеш-значения |
| CryptSignHash CryptVerifySignature | Получение и проверка ЭЦП |
| CryptGenRandom | Генерация случайного зна­чения |

При создании приложения на языке С++ в системах программи­рования Borland С++ Builder и Microsoft Visual С++ для доступа к прототипам этих функций, а также к определениям констант и ти­пов данных, используемых в CryptoAPI 1.0, потребуется заголовоч­ный файл wincrypt.h. При использовании Microsoft Visual С++ опе­ратор #include для подключения этого файла можно поместить в автоматически создаваемый конструктором приложений (AppWizard) файл stdafx.h (перед заключительным оператором #endіf). При ис­пользовании Borland С++ Builder файл wincrypt.h подключается автоматически.

*Получение информации о криптопровайдерах*

Приложение может получить следующую информацию.

1**.** Об установленных в системе криптопровайдерах:

* тип криптопровайдера (числовое значение и, возможно, тексто­вое описание);
* название криптопровайдера;
* список имен поддерживаемых криптоалгоритмов;
* список имен созданных контейнеров ключей.

2. Для каждого алгоритма, поддерживаемого криптопровайдером:

* тип алгоритма (шифрования данных или сообщений, ЭЦП, об
* мена сеансовыми ключами, хеширования);
* для алгоритмов шифрования - поддерживаемую длину ключей (значение по умолчанию, минимальное и максимальное значение);
* для алгоритмов хеширования - длину хеш-значения;
* для алгоритмов ЭЦП и обмена сеансовыми ключами - шаг из­менения длины ключа;
* для алгоритмов блочного шифрования - длину блока.

3.Для каждого созданного криптопровайдером контейнера ключей можно определить:

* созданы ли в нем пары ключей ЭЦП и обмена;
* какие права доступа к этому контейнеру ключей имеют различ­ные Пользователи системы (только для операционных систем Win­dows NT / 2000 / ХР / 2003).

Для получения этой информации предназначены следующие функции CryptoAPI 1.0:

BOOL WINAPI CryptEnumProviderTypes(DWORD dwlndex, DWORD \*pdwReserved, DWORD dwFlags, DWORD \*pdwProvType, LPTSTR pszTypeName, DWORD \*pcbTypeName); /\* получение информации о типе криптопровайдера с относительным номером dwlndex: число­вом значении (\*pdwProvType), описании (pszTypeName), длине строки с описанием (\*pcbTypeName); pdwReserved=NULL, dwFlags=0; если криптопровайдера с таким относительным номером нет, то функция возвращает FALSE, а вызванная сразу после нее функция GetLastError - ERROR\_NO\_MORE\_ITEMS; если криптопровайдер не поддерживает получение описания своего типа, то в параметре \*pcbTypeName возвращается 0. \*/

BOOL WINAPI CryptEnumProviders(DWORD dwlndex, DWORD \*pdwReserved, DWORD dwFlags, DWORD \*pdwProvType, LPTSTR pszProvName, DWORD \*pcbProvName); получение информации о криптопровайдере с относительным номером dwlndex; числовом значении типа (\*pdwProvType), имени (pszProvName), длине имени (\*pcbProvName); pdwReserved = NULL, dwFlags = 0; если криптопровайдера с таким относительным номером нет, то функция воз­вращает FALSE, а вызванная сразу после нее функция GetLastError -ERROR\_NO\_MORE\_ITEMS. \*/

BOOL CryptAcquireContext(HCRYPTPROV \*phProv, LPCSTR pszContainer, LPCSTR pszProvider, DWORD dwProvType, DWORD dwFlags); /\* получение в \*phProv дескриптора криптопровайдера с именем pszProvider и типом dwProvType для существующего контейнера ключей pszContainer (dwFlags=0) или (если ранее вызванная функция CryptAcquireContext возвратила FALSE с кодом ошибки NTE\_BAD\_KEYSET от функции GetLastError; для создаваемого ново­го контейнера ключей (dwFlags= CRYPT\_NEWKEYSET); если dwFlags=CRYPT\_VERIFYCONTEXT, то приложение не будет иметь доступа к секретным ключам асимметричного шифрования в кон­тейнере (значение pszContainer в этом случае должно быть уста­новлено в NULLj; если dwFlags=CRYPT\_DELETEKEYSET, то контей­нер ключей в криптопровайдере будет удален (значение параметра \*phProv при этом не определено); функция возвращает TRUE при успешном завершении и FALSE - в случае ошибки. \*/

Если при вызове функции CryptAcquireContext не указывается имя контейнера ключей (параметр pszContainer), то подразумевается кон­тейнер с именем по умолчанию. Встроенные в операционную систему Windows криптопровайдеры в качестве имени контейнера ключей по умолчанию используют имя учетной записи пользователя, от лица которого выполняется данное приложение. Хранение секретных клю­чей в контейнерах с именами по умолчанию ненадежно, так как одно приложение может разрушить ключи, созданные другой прикладной программой.

Если параметр dwFlags не содержит значения CRYPT\_MACHINE\_KEYSET, то встроенные в Windows криптопро­вайдеры хранят создаваемый или ищут открываемый контейнер клю­чей в профиле выполнившего эту операцию пользователя (в разделе реестра HKEY\_CURRENT\_USER). Если параметр dwFlags содержит значение CRYPT\_MACHINE\_KEYSET, то встроенные в Windows крип­топровайдеры хранят создаваемый или ищут открываемый контейнер ключей в разделе реестра HKEY\_LOCAL\_MACHINE. Это может по­требоваться, если пользователь получает доступ к контейнеру ключей с помощью системной службы или не входит в систему интерактивно.

Если параметр dwFlags содержит значение CRYPT\_VERIFYCONTEXT, то пользователь получает доступ к контейнеру ключей только для работы с открытым ключом (для проверки ЭЦП или экспорта сеансового ключа шифрования) и хеширования. BOOL WINAPI CryptGetProvParam(HCRYPTPROV hProv, DWORD dwParam, BYTE pbData, DWORD pdwDataLen, DWORD dwFlags); /\* получение информации о криптопровайдере с дескриптором hProv: именах созданных в нем контейнеров ключей (dwParam=PP\_ENUMCONTAINERS, dwFlags устанавливается в CRYPT\_FIRST для первого контейнера и 0 для всех следующих), именах и характеристиках реализованных криптоалгоритмов (dwParam=PP\_ENUMALGS\_EX, dwFlags устанавливается в CRYPT\_FIRST для первого алгоритма и 0 для всех следующих), ша­ге изменения длины асимметричного ключа обмена в битах (dwParam= PP\_KEYX\_KEYSIZE\_INC), шаге изменения длины ключа ЭЦП в битах (dwParam=PP\_SIG\_KEYSIZE\_INC), дескрипторе безо­пасности контейнера ключей (dwParam=PP\_KEYSET\_SEC\_DESCR, только для Windows NT/2000/ХР/2003) со сведениями о создателе контейнера (dwFlags = OWNER\_SECURITY\_INFORMATION) и правах доступа к нему различных субъектов (dwFlags= =DACL\_SECURITY\_INFORMATION) и др.; запрашиваемая инфор­мация помещается в буфер pbData длиной \*pdwDataLen; функ­ция возвращает TRUE при успешном завершении и FALSE е случае ошибки (при достижении конца списка имен контейнеров ключей или криптоалгоритмов функция GetLastError возвраща­ет ERROR\_NO\_MORE\_ITEMS. \*/

Структура буфера с информацией возвращаемой функцией CryptGetProvParam зависит от ее типа:

* если запрашивается информация о контейнерах ключей, то их имена помещаются в строку символов, оканчивающуюся 0;
* если запрашивается информация о реализованных криптоалго­ритмах, то она помещается в структуру типа PROV\_ENUMALGS\_EX, имеющую поля:

ALGJD aiAlgid; // код алгоритма

DWORD dwDefaultLen; // длина ключа по умолчанию

DWORD dwMinLen; // минимально возможная длина ключа

DWORD dwMaxLen; // максимально возможная длина ключа

DWORD dwProtocols; // количество реализованных криптоалгорит­мов и протоколов

DWORD dwNameLen; // длина сокращенного названия алгоритма

CHAR szName[20]; // сокращенное название алгоритма

DWORD dwLongNameLen; // длина полного названия алгоритма

GHAR szLongName[40]; // полное название алгоритма

3) если запрашивается информация о шаге изменения длины асимметричных ключей, то она возвращается в переменной типа DWORD.

Для определения типа криптоалгоритма по его коду следует ис­пользовать макрос GET\_ALG\_CLASS, который может возвращать зна­чения ALG\_CLASS\_HASH (хеширование), ALG\_CLASS\_SIGNATURE (получение и проверка ЭЦП), ALG\_CLASS\_KEY\_EXCHANGE (обмен сеансовыми ключами), ALG\_CI\_ASS\_DATA\_ENCRYPT (шифрование произвольных данных), ALG\_CLASS\_MSG\_ENCRYPT (шифрование сообщений в формате ASN.1).

Для алгоритмов хеширования вместо длины ключа возвраща­ется длина хеш-значения.

*Получение информации о криптографических ключах*

Определение длины блока и других параметров криптографи­ческого ключа возможно после его создания функцией CryptGenKey, которая будет рассмотрена в следующем разделе, с помощью функции CryptGetKeyParam.

BOOL WINAPI CryptGetKeyParam(HCRYPTKEY hKey, DWORD dwParam, BYTE \*pbData, DWORD \*pdwDataLen, DWORD dwFlags); Г получение параметров ключа с дескриптором hKey, полученном по­сле выполнения функции CryptGenKey: длины блока сеансового клю­ча (dwParam= KP\_BLOCKLENj, фактической длины ключа с учетом битов четности (dwParam=KP\_KEYLEN, для алгоритмов DES, 3-DES и 3-DES Two Key будет соответственно возвращаться 64, 192 и 128 бит), добавляемых к ключу симметричного шифрования слу­чайных значений (dwParam=KP\_SALT/), вектора инициализации для некоторых режимов алгоритмов симметричного шифрования (dwParam = KPJVj, режима симметричного шифрования (dwParam=KP\_MODE, поддерживаются значения CRYPT\_MODE\_CBC, CRYPT\_MODE\_CFB, CRYPT\_MODE\_ECB и CRYPT\_MODE\_OFB, по­следний режим не поддерживается встроенными в Windows крипто-провайдерами), длины порции данных в режимах симметричного шифрования с использованием регистра замены (tiwParam= =KP\_MODE\_BITSj, эффективной длины сеансового ключа (dwParam=KP\_EFFECTIVE\_KEYLEN, равной количеству случайных битов ключа) и др.; dwFlags=0; запрашиваемая характеристика воз­вращается в 6yqbepe\*pbData длиной \*pdwDataLen; функция возвраща­ет TRUE при успешном завершении и FALSE в случае ошибки. \*/

Структура буфера зависит от типа запрашиваемой с помощью функции CryptGetKeyParam информации: если запрашивается добав­ляемое к ключу случайное значение или вектор инициализации, то возвращается массив байт, а в остальных случаях, как правило, воз­вращается значение типа DWORD.

Для освобождения дескриптора криптопровайдера, полученного с помощью функции CryptAcquireContext, предназначена следую­щая функция CryptoAPI 1.0:

BOOL CryptReleaseContext(HCRYPTPROV hProv, DWORD dwFlags); /\* освобождение дескриптора криптопровайдера hProv (dwFlags=0) \*/

Рассмотрим пример получения информации о криптопровайдерах и реализованных ими криптоалгоритмах в программе на языке С++, созданной в системе программирования Borland С++ Builder. Окно, в котором будет отображаться получаемая информация, при­ведено на рис. 2.

На глобальном уровне объявим следующие переменные:

DWORD Len; // длина буфера для получения информации

char pTN[MAX\_PATH]; // описание типа криптопровайдера

DWORD рТуре, рТ[МАХ\_РАТН]; // тип и имя криптопровайдера

HCRYPTPROV hP=0; // дескриптор криптопровайдера

ALG\_ID рА[МАХ\_РАТН]; // коды криптоалгоритмов

UINT і; // относительный номер криптопровайдера

DWORD Def[MAX\_PATH], Min[MAX\_PATH], Мах[МАХ\_РАТН]; /\* длина ключа: по умолчанию, минимальная и максимальная \*/

AnsiString Tmp; // вспомогательная строка HCRYPTKEY hK=0; // дескриптор ключа

LPVOID MsgBuf; /\* указатель на буфер с текстом сообщения об ошибке \*/

При создании окна выполним следующий код:

AnsiString cpt; // вспомогательная строка

// установка длины буфера Len=sizeof(pTN);

// подготовка к получению типов криптопровайдеров

i=0;

// цикл получения информации о типах криптопровайдеров

while(CryptEnumProviderTypes(i,NULL,0,&pT[i],pTN,&Len)&&GetLastError()!=ERROR\_NO\_MORE\_ITEMS)

{ // если описание типа доступно

if(Len) Tmp=AnsiString(pTN)+cpt.sprintf(" (%d)",pT[i]);

// если описание типа недоступно

else Tmp.printf("(%d)",pT[i]);

/\* добавление информации о типе к списку «Типы криптопро­вайдеров»\*/

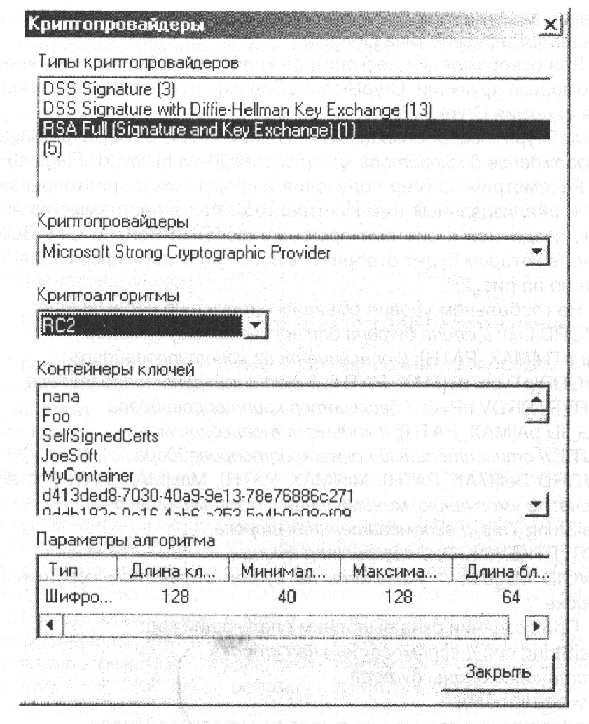


Рисунок 2 – Окно программы для получения информации о криптопровайдерах

Туреs->Items->Аdd(Тmр);

// увеличение индекса типа криптопровайдера

i++;

// установка длины буфера

Len=sizeof(pTN); }

// установка длины буфера

Len=sizeof(pTN);

// подготовка к получению имен криптопровайдеров

i=0;

// цикл получения имен криптопровайдеров while(CryptEnumProviders(i,NULL,0,&pT[i],pTN,&Len) && Len)

{ // добавление имени к списку «Криптопровайдеры»

Names->ltems->Add(pTN);

// увеличение индекса криптопровайдера

i++;

// установка длины буфера Len=sizeof(pTN); }

В обработку изменения выбора в списке «Криптопровайдеры» поместим код:

PROV\_ENUMALGS\_EX pAlg; // информация о криптоалгоритме

AnsiString nt; // описание типа

int j; // индекс типа криптоалгоритма

// сброс дескриптора криптопровайдера

if(hP) CryptReleaseContext(hP,0);

hP=0;

/\* очистка списков «Криптоалгоритмы», «Контейнеры ключей» и «Параметры алгоритма» \*/

Algs->Clear();

Conts->Clear();

Key->ltems->Clear();

// получение типа выбранного провайдера

pType=pT[Names-ltemlndex];

// установка длины буфера

Len=sizeof(pAlg);

// получение дескриптора выбранного криптопровайдера

if(!CryptAcquireContext(&hP,NULL,Names->Text.c\_str(),pType,0))

CryptAcquireContext(&hP,NULL,Names->Text.c\_str(),pType, CRYPT\_VERIFYCONTEXT);

/\* разрешение выбора в списках «Криптоалгоритмы» и «Контей­неры ключей» \*/

Algs->Enabled=true;

Conts->Enabled=true;

/\* получение строки для поиска в списке «Типы криптопровайде­ров»\*/

Tmp.printf("(%d)",pType);

// поиск в списке «Типы криптопровайдеров»

for(j=0;j<Types->ltems->Count;j++)

{ nt=Types->ltems->Strings[j];

if(nt.Pos(Tmp)) break; }

// выделение строки в списке «Типы криптопровайдеров»

if(j<Types->Items->Count) Types->Itemlndex=j;

// начало получения информации о криптоалгоритмах

i=0;

// цикл получения информации о крипто алгоритмах

if(CryptGetProvParam(hP,PP\_ENUMALGS\_EX,(BYTE\*)&pAlg,&Len, CRYPT\_FIRST))

do

{ // добавление имени к списку «Криптоалгоритмы»

Algs->ltems->Add(pAlg.szName);

// сохранение информации об очередном алгоритме

pA[i]=pAlg.aiAlgid;

Def[i]=pAlg.dwDefaultLen;

Min[i]=pAlg.dwMinLen;

Max[i]=pAlg.dwMaxLen;

// увеличение индекса алгоритма

i++;

// установка длины буфера

Len=sizeof(pAlg); }

while(CryptGetProvParam(hP,PP\_ENUMALGS\_EX, (BYTE\*)&pAlg,&Len,0));

/\* вывод сообщения об ошибке, если информация об алгоритмах недоступна \*/

else

{FormatMessage(FORMAT\_MESSAGE\_ALLOCATE\_BUFFER |

FORMAT\_MESSAGE\_FROM\_SYSTEM, NULL,

GetLastError(),

MAKELANGID(LANG\_NEUTRAL,SUBLANG\_DEFAULT),

(LPTSTR)&MsgBuf,0,NULL);

ShowMessage(AnsiString("Ошибка при получении информации об алгоритмах :\n") +(char\*)MsgBuf); LocalFree(MsgBuf);

// запрет выбора в списке «Криптоалгоритмы»

Algs->Enabled=false;}

// установка длины буфера

Len=sizeof(pTN);

// цикл получения информации о контейнерах ключей

if(!CryptGetProvParam(hP,PP\_ENUMCONTAINERS,pTN, &Len,CRYPT\_FIRST))

/\* вывод сообщения об ошибке, если информация о контейнерах недоступна \*/

FormatMessage(FORMAT\_MESSAGE\_ALLOCATE\_BUFFER | FORMAT\_MESSAGE\_FROM\_SYSTEM,

NULL,GetLastError(),

MAKELANGID(LANG\_NEUTRAL, SUBLANG\_DEFAULT),

(LPTSTR) &MsgBuf,0,NULL);

ShowMessage(AnsiString( "Ошибка при получении информации о контейнерах :\n") +(char\*)MsgBuf); LocalFree(MsgBuf);

// запрет выбора в списке «Контейнеры ключей» Conts->Enabled=false;}

else do

{ // добавление имени к списку «Контейнеры ключей»

Conts->ltems->Add(pTN);

// установка длины буфера

Len=size6f(pAlg); }

while(CryptGetProvParam(hP,PP\_ENUMCONTAINERS,pTN, &Len,0));

Если криптопровайдер хранит контейнер ключей на смарт-карте, а устройство для чтения смарт-карт не установлено, то ин­формация о контейнере не может быть получена. Если у пользова­теля, от чьего имени выполняется программа, нет никаких прав доступа к контейнеру ключей, то выводится соответствующее со­общение. На рис. 3 приведены примеры сообщений об ошибках при получении информации о криптопровайдерах.

В обработку изменения выбора в списке «Криптоалгоритмы» поместим код:

TListltem \*item; // элемент списка «Параметры алгоритма»

DWORD at.bl; // тип алгоритма и длина блока

// получение кода выбранного алгоритма

ALGJD ai=pA[Algs->ltemlndex];

// очистка списка «Параметры алгоритма»

Key->ltems->Clear();

// добавление элемента к списку «Параметры алгоритма» item=Key->ltems->Add();

/\* определение и отображение информации о типе выбранного алгоритма \*/

if(GET\_ALG\_CLASS(ai)==ALG\_CLASS\_HASH)

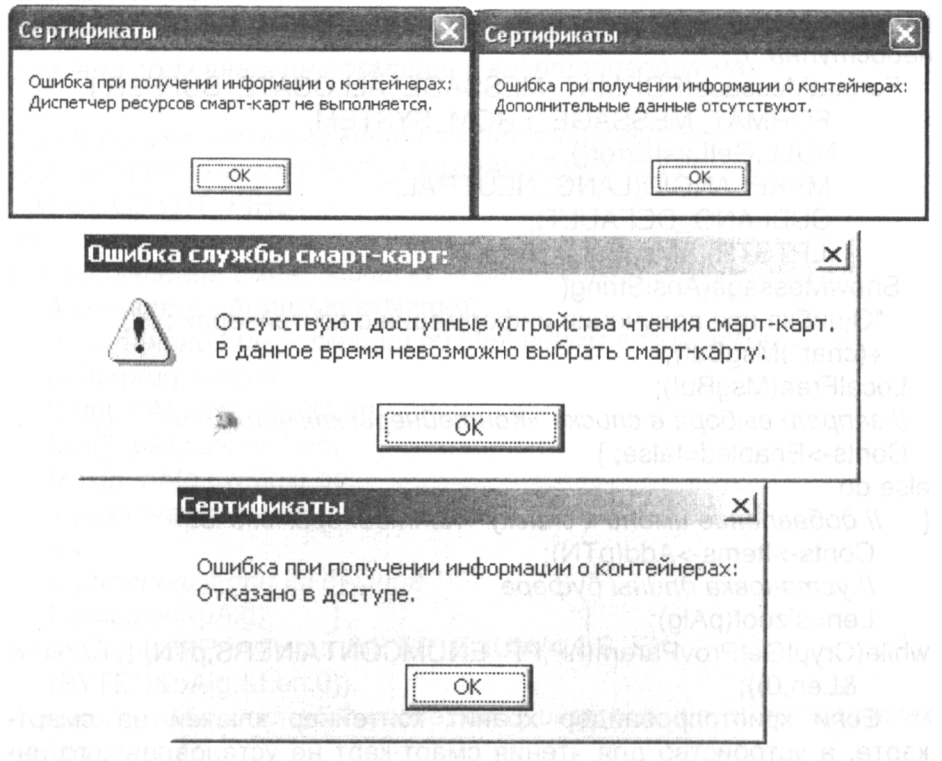


Рисунок 3 – Сообщения об ошибках при получении информации о контейнерах ключей

iiem->Caption="XeujHpoBaHHe";

else lf(GET\_ALG\_CLASS(ai)==ALG\_CLASS\_SIGNATURE)

item->Caption="ЭЦП";

else lf(GET\_ALG\_CLASS(ai)~ALG\_CLASS\_KEY\_EXCHANGE)

item->Caption ="Обмен сеансовыми ключами";

else if(GET\_ALG\_CLASS(ai)==ALG\_CLASS\_DATA\_ENCRYPT)

item->Caption ="Шифрование данных";

else if(GET\_ALG\_CLASS(ai)==ALG\_CLASS\_MSG\_ENCRYPT)

item->Caption ="Шифрование сообщений";

else item->Caption ="Неизвестный";

if(item->Caption!="Hen3BecTHb^")

// получение и отображение информации о длинах ключа

{item->Subltems->Add(Def[Algs->ltemlndex]);

item->Subltems->Add(Min[Algs->ltemlndex]);

item->Subltems->Add(Max[Algs->ltemlndexj);

// установка длины буфера

Len=sizeof(at);

/\* получение и отображение информации о шаге изменения дли­ны ключа алгоритмов ЭЦП и обмена сеансовыми ключами \*/

Key->Columns->ltems[4]->Caption="lllar изменения длины";

if(GET\_ALG\_CLASS(ai)==ALG\_CLASS\_SIGNATURE)

if(CryptGetProvParam(hP,PP\_SIG\_KEYSIZE\_INC,(BYTE\*)&at,&Len,0))

item->Subltems->Add(at); else;

else if(GET\_ALG\_CLASS(ai)==ALG\_CLASS\_KEY\_EXCHANGE)

if(CryptGetProvParam(hP,PP\_KEYX\_KEYSIZE\_INC,(BYTE\*)&at,&Len,0))

item->Subltems->Add(at); else;

/\* получение и отображение информации о длине блока сеансо­вого ключа \*/

else if(GET\_ALG\_CLASS(ai)==ALG\_CLASS\_DATA\_ENCRYPT)

{// освобождение дескриптора ранее созданного ключа

if(hK) CryptDestroyKey(hK);

Key->Columns->ltems[4]->Caption="flnnHa блока";

// создание случайного сеансового ключа

if(CryptGenKey(hP,ai,0,&hK))

{// установка длины буфера Len=sizeof(bl);

if(CryptGetKeyParam(hK,KP\_BLOCKLEN,(BYTE\*)&bl,&Len,0))

item->Subltems->Add(bl);} else

{

// вывод сообщения об ошибке при получении длины блока

FormatMessage( FORMAT\_MESSAGE\_ALLOCATE\_BUFFER |

FORMAT\_MESSAGE\_FROM\_SYSTEM, NULL,

GetLastError(),

MAKELANGID(LANG\_NEUTRAL, SUBLANG\_DEFAULT),

(LPTSTR) &MsgBuf,0,NULL);

ShowMessage(AnsiString( "Ошибка при получении длины блока:\n")+ (char\*)MsgBuf);

LocalFree(MsgBuf); } }

/\* очистка заголовка последнего столбца списка «Параметры алгоритмов» для алгоритмов хеширования и шифрования сооб­щений \*/

else

if(GET\_ALG\_CLASS(ai)==ALG\_CLASS\_HASH ||

GET\_ALG\_CLASS(ai)==ALG\_CLASS\_MSG\_ENCRYPT)

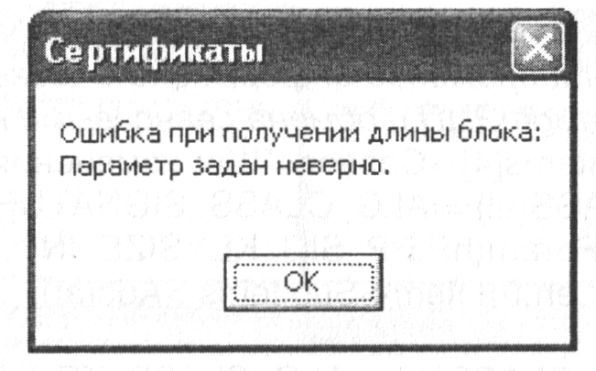


Рисунок 4 –Сообщение об ошибке при получении информации о криптоалгоритме

Key->Columns->ltems[4]->Caption=""; }

Некоторые криптопровайдеры неправильно обрабатывают за­прос на получение информации о длине блока, поэтому при выпол­нении этой программы может выводиться сообщение об ошибке (рис. 4).

*Создание, хранение и распространение криптографических ключей*

Большинство криптопровайдеров не создают автоматически пары ключей асимметричного шифрования при создании контейне­ра ключей.

1. Для создания пар ключей асимметричного шифрования

должна использоваться следующая функция CryptoAPI:

BOOL CryptGenKey(HCRYPTPROV hProv, ALGJD Algid, DWORD dwFlags, HCRYPTKEY \*phKey); /\* создание в контейнере ключей с дескриптором hProv пары ключей ЭЦП (Algid=AT\_SIGNATURE) или обмена сеансовыми ключами (Algid=AT\_KEYEXCHANGE) и запись дескриптора открытого ключа созданной пары в \*phKey; если секретный ключ созданной пары должен иметь возможность экс­порта из CSP, то dwFlags=CRYPT\_EXPORTABLE (открытые ключи всегда являются экспортируемыми). \*/

2. Получение дескриптора открытого ключа \*phUserKey из соот-

ветствующего контейнера ключей hProv возможно с помощью

функции:

BOOL CryptGetUserKey(HCRYPTPROV hProv, DWORD dwKeySpec, HCRYPTKEY \*phUserKey); I\* параметр dwKeySpec определяет тип запрашиваемого ключа - обмена (AT\_KEYEXCHANGE,) или ЭЦП fAT\_SIGNATURE; \*/

Если функция CryptGetUserKey возвращает FALSE с кодом ошибки NTE\_NO\_KEY, то запрашиваемый открытый ключ в контей­нере ключей криптопровайдера с дескриптором hProv не существу­ет и соответствующая пара ключей асимметричного шифрования (для обмена сеансовыми ключами или ЭЦП) должна быть создана с помощью функции CryptGenKey.

3. Сеансовый ключ можно создать двумя способами. При первом способе используется функция CryptGenKey со значением параметра Algid, равным коду алгоритма используемого в приложении симмет­ричного шифрования (CALG\_DES, CALG\_RC2, CALG\_3DES, CALG\_RC4 или др.). Значение параметра dwFlags может быть объе­динением следующих флагов: CRYPT\_CREATE\_SALT (использование случайного значения для модификации ключа шифрования), CRYPT\_EXPORTABLE (сеансовый ключ может экспортироваться из CSP) и др.

При создании ключа может быть задана его длина, отличаю­щаяся от длины по умолчанию. В этом случае параметр dwFlags при вызове функции CryptGenKey должен в комбинации с другими допустимыми флагами содержать значение типа DWORD, старшие 16 бит которого содержат требуемую длину ключа (например, для задания длины ключа ЭЦП 2048 бит нужно указать значение 0x08000000).

Другим способом создания сеансового ключа симметричного шифрования является его генерация из хеш-значения введенной пользователем ключевой фразы. В этом случае используются сле­дующие функции CryptoAPI:

BOOL CryptCreateHash(HCRYPTPROV hProv, ALGJD Algid, HCRYPTKEY hKey, DWORD dwFlags, HCRYPTHASH \*phHash); /\* создание в криптопровайдере с дескриптором hProv пустого хеш-значения с дескриптором \*phHash (в Algid, должен содер­жаться код алгоритма хеширования – CALG\_MD2, CALG\_MD4, CALG\_MD5 или CALG\_SHA, параметры hKey и dwFlags не исполь­зуются и должны быть равны нулю. \*/

BOOL CryptHashData(HCRYPTHASH hHash, CONST BYTE \*pbData, DWORD dwDataLen, DWORD dwFlags); /\* добавление к хеш-значению с дескриптором hHash данных (например, парольной фразы) из буфера \*pbData длиной dwDataLen; параметр dwFlags не используется и должен быть равен нулю. \*/

BOOL CryptDeriveKey(HCRYPTPROV hProv, ALGJD Algid, HCRYP­THASH hBaseData, DWORD dwFlags, HCRYPTKEY \*phKey); /\* соз­дание сеансового ключа с дескриптором \*phKey из хеш-значения с дескриптором hBaseData; значения параметров Algid (код алго­ритма шифрования) и dwFlags (флаги) могут быть такими же, как при вызове функции CryptGenKey. \*/

После вызова функции CryptDeriveKey в используемое ею хеш-значение не могут быть добавлены новые данные. После заверше­ния работы с хеш-значениями и ключами шифрования их дескрип­торы должны быть разрушены (занимаемая ими оперативная па­мять освобождена) в приложении с помощью следующих функций:

BOOL CryptDestroyKey(HCRYPTKEY hKey); /\* разрушение дескрип­тора ключа шифрования hKey. \*/

BOOL CryptDestroyHash(HCRYPTHASH hHash); /\* разрушение де­скриптора хеш-значения hHash \*/

Пример. Приведем пример использования функции CryptGetUserKey для определения факта создания пар ключей асимметричного шифрования в контейнере (это будет дополнени­ем к примеру, рассмотренному в предыдущем разделе).

Добавим следующий код в обработку изменения выбора в спи­ске «Контейнеры ключей» (см. рис. 2):

// получение имени выбранного контейнера

AnsiString pN=Conts->ltems->Strings[Conts->ltemlndex];

bool flag=false; // признак создания ключей

/\* освобождение ранее полученного дескриптора криптопровайдера \*/

if(hP) CryptReleaseContext(hP,0);

/\* получение дескриптора к,иптопровайдера для выбранного контейнера ключей \*/

if(CryptAcquireContext(&hP,pN.c\_str(),

Names->Text.c\_str(),pType,0))

{ /\* начало подготовки к формированию сообщения о результа­тах проверки 7

Тmр="В контейнере "+pN+":\n";

// освобождение дескриптора ранее созданного ключа

if(hK) CryptDestroyKey(hK);

// проверка создания ключей ЭЦП

if(CryptGetUserKey(hP,AT\_SIGNATURE,&hK))

{ Тmр+="есть пара ключей ЭЦП \n";

flag=true; }

// проверка создания ключей обмена

if(CryptGetUserKey(hP,AT\_KEYEXCHANGE,&hK))

{ Тmр+="есть пара ключей обмена \n";

flag=true; }

if (!flag) Тmр+="не созданы ключи" ;

// вывод сообщения о результатах проверки

ShowMessage(Tmp); }

/\* обработка ошибок при открытии контейнера ключей и вывод сообщения \*/

else

{ FormatMessage(FORMAT\_MESSAGE\_ALLOCATE\_BUFFER|

FORMAT\_MESSAGE\_FROM\_SYSTEM,NULL,GetLastError(),

MAKELANG ID(LANG\_NEUTRAL,SUBLANG\_DEFAULT),

(LPTSTR) &MsgBuf,0,NULL);

ShowMessage(AnsiString( "Ошибка при получении информации о контейнере:") +pN+":\n")+(char\*)MsgBuf); LocalFree(MsgBuf);

/\* получение дескриптора криптопровайдера без доступа к сек­ретному ключу (в режиме проверки) \*/

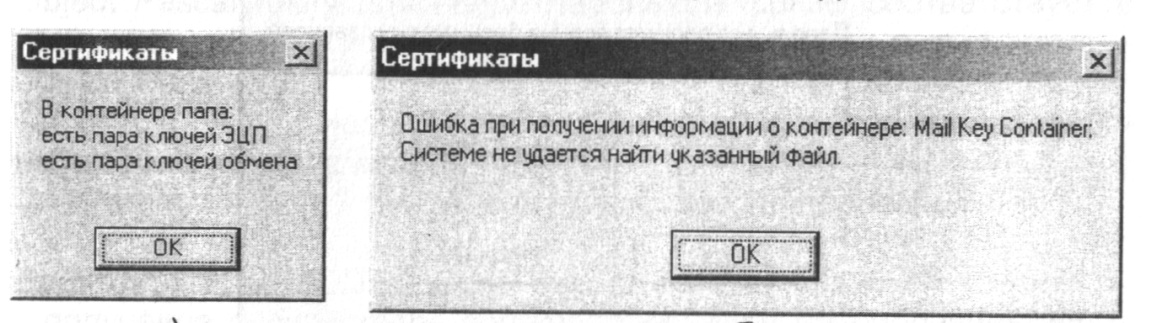
CryptAcquireContext(&hP,NULL,Names->Text.c\_str(),pType,

CRYPT\_VERIFYCONTEXT); }

На рис. 5 приведены пример окна с сообщением о результа­тах проверки создания пар ключей в одном из контейнеров (рис. 5,а) и пример вывода сообщения о невозможности получения информации о контейнере ключей (рис. 5,6).

Для изменения режима симметричного шифрования (ECB, СВС, CFB или OFB) используется функция CryptSetKeyParam: BOOL CryptSetKeyParam(HCRYPTKEY hKey, DWORD dwParam, BYTE \*pbData, DWORD dwFlags); Л установка режима шифрова­ния для сеансового ключа с дескриптором hKey; dwParam = =KP\_MODE, pbData указывает на переменную типа DWORD (un­signed long), в которой записан код устанавливаемого режима, dwFlags = 0 \*/

По умолчанию режим шифрования устанавливается в CRYPT\_MODE\_ СВС. Функция CryptSetKeyParam может также при­меняться и для установки других параметров шифрования:



а) б)

Рисунок 5. Примеры сообщений с информацией о контейнере ключей

использование вектора инициализации (синхропосылки) -dwParam = KP\_IV, а в буфер \*pbData нужно поместить значение вектора инициализации;

использование случайных значений для модификации ключа шифрования - параметр dwParam - KP\_SALT, а в буфер \*pbData нужно поместить случайное значение;

размер порции данных для режимов шифрования с обратной связью CFB или OFB - параметр dwParam = KP\_MODE\_BITS , а в буфер \*pbData нужно поместить длину порции данных (для встро­енных в Windows криптопровайдеров Microsoft это значение по умолчанию равно 8);

дополнительные ограничения на использование сеансового ключа -параметр dwParam=KP\_PERMISSIONS и в буфер \*pbData нужно по­местить комбинацию флагов CRYPT\_ENCRYPT (разрешено шифро­вание на этом ключе), CRYPT\_DECRYPT (разрешено расшифрование с помощью этого ключа), CRYPT\_EXPORT (ключ может экспортиро­ваться из CSP), CRYPT\_READ (параметры ключа могут быть прочита­ны), CRYPT\_WR!TE (параметры ключа могут быть изменены), CRYPT\_MAC (ключ может использоваться для вычисления кода ау­тентификации сообщений); встроенные в Windows криптопровайдеры поддерживают только флаг CRYPT\_EXPORT.

Пример. Рассмотрим пример создания ключа шифрования файла на основе введенной парольной фразы в программе на язы­ке С++, созданной в системе программирования Microsoft Visual С++. Парольная фраза вводится с помощью диалогового окна (рис. 6), которому в приложении соответствует объект Dialog6.

С текстовым редактором для ввода пароля в классе этого объ­екта связано строковое поле m\_Edit1.

На глобальном уровне объявим переменные:

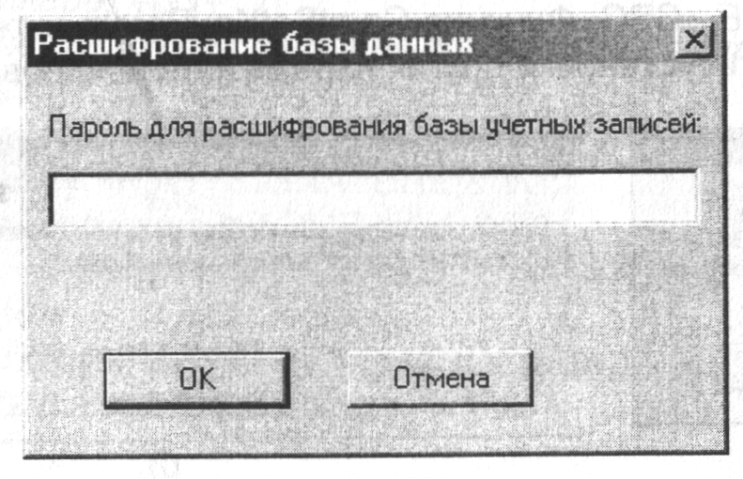


Рисунок 6 – Окно ввода парольной фразы

HCRYPTPROV hProv=0; // дескриптор криптопровайдера

HCRYPTKEY hKey; // дескриптор ключа шифрования (расшифро­вания)

HCRYPTHASH hHash; // дескриптор хеш-значения

DWORD Param=CRYPT\_MODE\_CBC;// режим симметричного шифрования

В месте, где необходимо создание сеансового ключа, поместим код:

/\* получение дескриптора криптопровайдера по умолчанию типа PROV\_RSA\_FULL для контейнера ключей с именем по умолчанию (при необходимости создание контейнера) \*/

if(!CryptAcquireContext(&hProv,NULL,NULL,PROV\_RSA\_FULL,0))

if((unsigned)GetLastError()==NTE\_BAD\_KEYSET)

CryptAcquireContext(&hProv, NULL, NULL, PROV\_RSA\_FULL, CRYPT\_NEWKEYSET);

// создание пустого хеш-значения

CryptCreateHash(hProv,CALG\_SHA.O,0,&hHash);

// хеширование парольной фразы

CryptHashData(hHash,

(BYTE\*)Dialog6.m\_Edit1.GetBuffer(

Dialog6.m\_Edit1 .GetLength()),

Dialog6.m\_Edit1 .GetLength(),0);

// генерация сеансового ключа

CryptDeriveKey(hProv,CALG\_RC2,hHash,CRYPT\_EXPORTABLE, &hKey);

// установка режима симметричного шифрования

CryptSetKeyParam(hKey,KP\_MODE,(BYTE\*)&Param,0);

// разрушение хеш-значения CryptDestroyHash(hHash);

Экспорт криптографического ключа заключается в его получе­нии внутри специального блока данных - блоба (от Bit Large OBject, BLOB) в открытом (тип блоба PUBLICKEYBLOB, предназначен для экспорта открытых ключей асимметричного шифрования) или за­шифрованном (типы блоба SIMPLEBLOB для экспорта сеансовых ключей или PRIVATEKEYBLOB для экспорта секретного и открыто­го ключей асимметричного шифрования). Ключом шифрования секретного ключа при его экспорте должен быть специальный се­ансовый ключ, обычно генерируемый на основе парольной фразы. Ключом шифрования экспортируемого сеансового ключа является открытый ключ получателя блоба с сеансовым ключом (т.е. лица с правами расшифрования зашифрованных на этом сеансовом клю­че данных). Для экспорта и импорта ключей шифрования предна­значены следующие функции CryptoAPI:

BOOL CryptExportKey(HCRYPTKEY hKey, HCRYPTKEY hExpKey, DWORD dwBlobType, DWORD dwFlags, BYTE \*pbData, DWORD \*pdwDataLen); /\* экспорт криптографического ключа с дескрип­тором hKey, зашифрованного с помощью ключа с дескриптором hExpKey, в блобе \*pbData длиной \*pdwDataLen типа dwBlobType; при успешном завершении в \*pdwDataLen помещается фактиче­ская длина блоба \*/

BOOL CryptlmportKey(HCRYPTPROV hProv, CONST BYTE \*pbData, DWORD dwDataLen, HCRYPTKEY hPubKey, DWORD dwFlags, HCRYPTKEY \*phKey); /\* расшифрование криптографического ключа из блоба \*pbData длиной dwDataLen с помощью ключа с де­скриптором hPubKey и импорт восстановленного ключа в контейнер ключей hProv; при успешном завершении в \*phKey поме­щается дескриптор импортированного ключа. \*/

Расшифрование импортируемого сеансового ключа выполняется с помощью секретного ключа получателя блоба, а импортируемого секретного ключа - с помощью специального сеансового ключа.

Если при шифровании используются вектор инициализации и (или) случайные ключевые значения, то эти данные могут быть за­писаны в конец (начало) шифротекста для использования при рас­шифровании. Если сеансовый ключ не генерируется из парольной фразы, а создается случайно, то в шифротекст должны быть также записаны блобы с этим ключом, зашифрованным открытыми клю­чами обмена всех пользователей, которые должны иметь доступ к этой зашифрованной информации.

Если к сеансовому ключу шифрования файла имеет доступ только один пользователь, то потеря (например, в результате про­граммной или аппаратной ошибки) пары ключей обмена этого пользователя может привести к невозможности восстановления зашифрованных данных. Для предотвращения подобной угрозы может использоваться процедура резервной авторизации:

после шифрования файла и экспорта сеансового ключа обычным образом сеансовый ключ экспортируется повторно с по­мощью открытого ключа резервной авторизации, а полученный блоб посылается сервису резервной авторизации вместе с описа­нием сеансового ключа и другой идентифицирующей информации;

при необходимости восстановления сеансового ключа и рас­шифрования файла потребуется сначала пройти аутентификацию у сервиса резервной авторизации.

Сервис резервной авторизации должен выполняться на защи­щенном (с помощью организационных и инженерно-технических методов) компьютере и предоставлять память для хранения сеан­совых ключей своих клиентов.

*Организация обмена*

Для организации обмена открытыми ключами асимметричного шифрования возможно как использование удостоверяющих центров, так и передача открытых ключей напрямую между пользователями:

отправитель экспортирует из криптопровайдера свой откры­тый ключ в форме блоба (типа PUBLICKEYBLOB) с помощью функ­ции Сгур1Ехро11Кеу;

блоб посылается получателю по защищенному каналу связи (например, в зашифрованном виде с помощью сеансового ключа, генерируемого из специальной парольной фразы, или в открытом виде с возможной конвертацией в текстовый формат);

3) получатель блоба импортирует его в свой криптопровайдер с помощью функции CryptlmportKey.

Для передачи сеансового ключа также могут применяться два способа. В первом случае отправитель создает случайный сеансо­вый ключ (с помощью функции CryptGenKey), зашифровывает его при помощи ранее полученного открытого ключа получателя (ис­пользуется функция CryptExportKey) в виде блоба типа SIMPLE-BLOB и отправляет блоб получателю, который расшифровывает сеансовый ключ с помощью своего секретного ключа обмена (ис­пользуется функция CryptlmportKey). Для снижения риска повтор­ной посылки нарушителем перехваченного им ранее блоба с сеан­совым ключом и зашифрованного с помощью этого ключа сообще­ния можно использовать отметки времени или последовательную нумерацию сообщений на основе случайного начального значения.

Другой способ передачи сеансового ключа заключается в ис­пользовании специального трехфазного протокола (предполагает­ся, что отправитель А и получатель В имеют открытые ключи обме­на РКА, РКВ и логические имена IDA, Юв друг друга):

Первая фаза протокола.

А: генерация случайного сеансового ключа kA (CryptGenKey); шифрование его с помощью открытого ключа В ЕРКВ (кд) (CryptEx­portKey).

А->В: Еркв (кд).

В: расшифрование блоба с сеансовым ключом кА=0ЗКв(Еркв (kA)) (CryptlmportKey).

Вторая фаза протокола:

В: генерация случайного сеансового ключа kB (CryptGenKey); шифрование его с помощью открытого ключа A ЕРКА (kB) (CryptEx­portKey).

В->А: ЕРКА (кв).

В: вычисление хеш-значения H1B=H(kA, Юв, кв, ЮА, «Фаза 2») (CryptCreateHash, CryptHashSessionKey, CryptHashData, CryptGetHashParam).

B->A: H1B.

А: расшифрование блоба с сеансовым ключом **k**B=DsKA(EpKA (kB)) (CryptlmportKey); вычисление H1A=H(kA, IDB, kB, IDA, «Фаза 2») (CryptCreateHash, CryptHashSessionKey, CryptHashData, CryptGetHashParam); сравнение H1B и H1A; при несовпадении хеш-значений (получатель не является подлинным или произошло ис кажение передаваемых по сети сообщений третьим лицом) выпол­нение протокола прекращается, а сеанс связи завершается. Третья фаза протокола.

А: вычисляет хеш-значение H2A=H(kB, IDA, IDB, «Фаза 3») (Crypt­CreateHash, CryptHashSessionKey, CryptHashData, CryptGetHash­Param).

A->B: H2A.

В: вычисление хеш-значение Н2в=Н(кв, IDA, IDB, «Фаза 3») (CryptCreateHash, CryptHashSessionKey, CryptHashData, CryptGetHashParam); сравнение H2A и H2B; при совпадении хеш-значений сеансовые ключи кА и кв могут использоваться для обме­на зашифрованными с их помощью сообщениями.

При выполнении данного трехфазного протокола потребуется использование еще двух функций CryptoAPI:

BOOL CryptHashSessionKey(HCRYPTHASH hHash, HCRYPTKEY hKey, DWORD dwFlags); /\* добавление в хеш-значение с дескрип­тором hHash сеансового ключа шифрования с дескриптором hKey; значение параметра dwFlags не используется и должно быть равно нулю \*/

BOOL CryptGetHashParam(HCRYPTHASH hHash, DWORD dwParam, BYTE \*pbData, DWORD \*pdwDataLen, DWORD dwFlags); /\* получе­ние в буфере \*pbData длиной \*pdwDataLen хеш-значения с деск­риптором hHash (dwParam=HP\_HASHVALJ; после завершения в \*pdwDataLen помещается действительный размер хеш-значения; значение параметра dwFlags не используется и должно быть равно нулю; после получения фактического хеш-значения добав­ление в него новых данных невозможно 7

Параметр dwParam может принимать еще два значения: HP\_HASHSIZE (в \*pbData будет содержаться размер в байтах хеш-значения) и HP\_ALGID (в буфер \*pbData будет помещен код ис­пользуемого алгоритма хеширования).

**Задание:**

1) Ознакомиться с теоретическими положениями, посвященными принципам работы с криптографическим интерфейсом Windows.

2) Написать программу которая обеспечивает:

* получение информации о криптопровайдерах и реализованных ими алгоритмах;
* обеспечивает создание сеансового ключа шифрования;
* обеспечивает создание пары ключей ассиметричного шифрования;
* проверяет факт создания ключей ассиметричного шифрования;

средствами CryptoAPI.

**Контрольные вопросы**

* Дайте определение понятию «Криптографический интерфейс».
* Перечислите принципы взаимодействия приложения и криптопровайдера.
* Какие атрибуты криптопровайдера вам известны?
* Какие типы криптопровайдеров Вы знаете?
* Перечислите основыне функции CryptoAPI 1.0.
* С помощью каких функции CryptoAPI можно получить информацию о криптопровайдере?
* Каким образом можно получить информацию о параметрах ключа?
* С помощью каких функций создаются ключи ассметричного шифровании? Ключ симметричного шифрования?
* Каким образом осуществяелтся экспорт и импорт ключей средствами CryptoAPI?
* Каким образом производится организация обмена открытыми ключами ассиметричного шифрования?

# Лабораторная работа 8 Антивирусные программные комплексы

**Цель занятия:** изучение способов защиты информации от вирусов на примере программы Антивирус Касперского

**Норма времени**: 2 часа

**Методическое обеспечение:** методические указания к практической работе

**Теоретические сведения**

**Компьютерный вирус** - программа способная самопроизвольно внедряться и внедрять свои копии в другие программы, файлы, системные области компьютера и в вычислительные сети, с целью создания всевозможных помех работе на компьютере.

Признаки заражения:

* прекращение работы или неправильная работа ранее функционировавших программ
* медленная работа компьютера
* невозможность загрузки ОС
* исчезновение файлов и каталогов или искажение их содержимого
* изменение размеров файлов и их времени модификации
* уменьшение размера оперативной памяти
* непредусмотренные сообщения, изображения и звуковые сигналы
* частые сбои и зависания компьютера и др.

**Классификация компьютерных вирусов**

*По среде обитания:*

* Сетевые – распространяются по различным компьютерным сетям
* Файловые – внедряются в исполняемые модули (COM, EXE)
* Загрузочные – внедряются в загрузочные сектора диска или сектора, содержащие программу загрузки диска
* Файлово-загрузочные – внедряются и в загрузочные сектора и в исполняемые модули

По способу заражения:

* Резидентные – при заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения
* Нерезидентные – не заражают оперативную память и активны ограниченное время

По воздействию:

* Неопасные – не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках
* Опасные – приводят к различным нарушениям в работе компьютера
* Очень опасные – могут приводить к потере программ, данных, стиранию информации в системных областях дисков

По особенностям алгоритма:

* Паразиты – изменяют содержимое файлов и секторов, легко обнаруживаются
* Черви – вычисляют адреса сетевых компьютеров и отправляют по ним свои копии
* Стелсы – перехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области
* Мутанты – содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую
* Трояны – не способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему

**Основные меры по защите от вирусов**

* оснастите свой компьютер одной из современных антивирусных программ: Doctor Web, Norton Antivirus, AVP
* постоянно обновляйте антивирусные базы
* делайте архивные копии ценной для Вас информации (гибкие диски, CD)

**Классификация антивирусного программного обеспечения**

* Сканеры (детекторы). Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов.
* Мониторы. Это целый класс антивирусов, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. С помощью монитора можно остановить распространение вируса на самой ранней стадии.
* Ревизоры. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Для определения наличия вируса в системе программы-ревизоры проверяют созданные ими образы и производят сравнение с текущим состоянием.

В 2009 году различные производители антивирусов стали сообщать о широком распространении нового типа программ — ложных или лжеантивирусов (rogueware).

По сути эти программы или вовсе не являются антивирусами (то есть не способны бороться с вредоносным ПО), или даже являются вирусами (воруют данные кредитных карт и т. п.). Ложные антивирусы используются для вымогательства денег у пользователей путём обмана. Один из способов заражения ПК ложным антивирусом следующий. Пользователь попадает на «инфицированный» сайт, который выдаёт ему предупреждающее сообщение вроде «На вашем компьютере обнаружен вирус» и предлагает скачать бесплатную программу для удаления вируса. После установки такая программа производит сканирование компьютера и якобы обнаруживает ещё массу вирусов. Для удаления вредоносного ПО ложный антивирус предлагает купить платную версию программы. Шокированный пользователь платит (суммы колеблются от $10 до $80) и ложный антивирус очищает ПК от несуществующих вирусов.

Антивирус Касперского - это классическая защита компьютера от вирусов, троянских и шпионских программ, а также от любого другого вредоносного ПО.

**Базовая защита:**

* Комплексная защита от всех видов вредоносных программ
* Проверка файлов, почтовых сообщений и интернет-трафика
* Защита интернет-пейджеров (ICQ, MSN). Улучшено!
* Автоматическое обновление баз

**Предотвращение угроз:**

* Проактивная защита от новых и неизвестных угроз
* Поиск уязвимостей в ОС и установленном ПО.
* Блокирование ссылок на зараженные сайты.
* Защита конфиденциальных данных:
* Блокирование ссылок на фишинговые сайты

**Дополнительные функции:**

* Защита от вирусов, троянских программ и червей
* Защита от шпионских и рекламных программ
* Проверка файлов в автоматическом режиме и по требованию
* Проверка почтовых сообщений (для любых почтовых клиентов)
* Проверка интернет-трафика (для любых интернет-браузеров)
* Защита интернет-пейджеров (ICQ, MSN)
* Проактивная защита от новых вредоносных программ
* Проверка Java- и Visual Basic-скриптов

Предотвращение угроз

* Поиск уязвимостей в ОС и установленном ПО
* Анализ и устранение уязвимостей в браузере Internet Explorer
* Блокирование ссылок на зараженные сайты
* Распознавание вирусов по способу их упаковки
* Глобальный мониторинг угроз (Kaspersky Security Network)
* Восстановление системы и данных:
* Возможность установки программы на зараженный компьютер
* Функция самозащиты программы от выключения или остановки
* Восстановление корректных настроек системы после удаления вредоносного ПО
* Наличие инструментов для создания диска аварийного восстановления

**Удобство использования:**

* Автоматическая настройка программы в процессе установки
* Готовые решения (для типичных проблем)
* Наглядное отображение результатов работы программы
* Информативные диалоговые окна для принятия пользователем обоснованных решений
* - Возможность выбора между простым (автоматическим) и интерактивным режимами работы
* Круглосуточная техническая поддержка
* Автоматическое обновление баз

**Ход работы**

После запуска приложения в системной панели появляется значок, вид которого зависит от состояния антивирусной защиты: включена ли постоянная защита и запущена ли проверка по требованию. Если постоянная защита включена, значок активен (красного цвета) 1, если выключена - неактивен (серого цвета) 1. Если запущена полная проверка компьютера, проверка отдельного файла, диска или выполняется анализ какого-либо объекта в режиме постоянной защиты, то на системной панели отображается мигающий значок 1. При проверке входящей почты появляется значок1 , а при ошибке запуска одной из задач постоянной защиты - 1. Во время загрузки обновлений антивирусных баз и модулей приложения значок меняется на 1.

**Настройка обновлений**

**1 способ**. В процессе установки Антивируса Касперского версии 6.0 Мастер первоначальной настройки предлагает настроить обновление антивирусных баз. Вы можете выбрать один из трех режимов расписания обновления:

**Автоматически** - процесс обновления самостоятельно проверяет свежие поступления на серверах обновлений **Лаборатории Касперского**, учитывая нагрузку на сервера. Специалисты **Лаборатории Касперского** рекомендуют использовать этот режим обновлений.

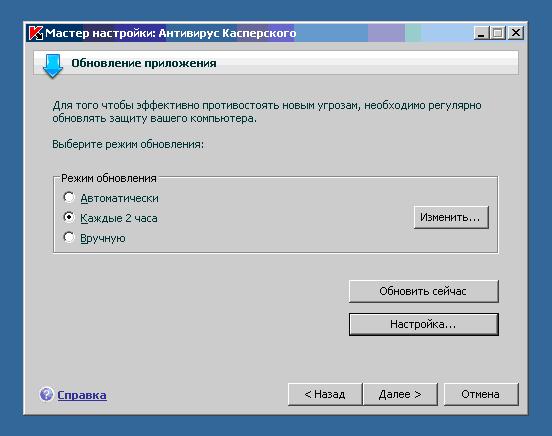
**Каждый 2 часа** - Вы можете самостоятельно установить расписание обновлений. Возможно задать не только расписание дней, но и часы, минуты, недели, месяцы.

**Вручную** - обновление стартует только по нажатии соответствующей кнопки в интерфейсе антивируса.

Нажав на кнопке **Обновить сейчас**, Вы можете немедленно обновить антивирусные базы еще до завершения процесса установки.

Нажав на кнопке **Настройка**, Вы можете задать вручную настройки прокси сервера, добавить или изменить источник обновления, а также задать учетную запись (логин\пароль) для процесса обновления.

Для начала выбираем Режим обновления (Автоматически, Каждые 2 часа или Вручную), затем задаем нужные нам настройки для случаев ручного Параметры LAN и источник обновления или периодической (график обновления) обновления

Задайте необходимые настройки и нажмите кнопку **Далее** для продолжения первоначальной настройки антивируса Касперского версии 6.0

**2 способ.** Для обновления сигнатур антивирусной программы в процессе работы, войдем на вкладку **Сервис** выберем **Обновить** и укажем путь, откуда будем считывать новые сигнатуры выбрав пункт **Настройка.**

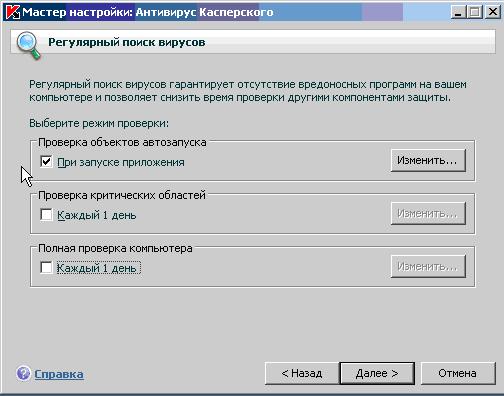
**Настройка проверки компьютера**

**1 способ**. В процессе установки Антивируса Касперского версии 6.0 Мастер первоначальной настройки предлагает настроить проверку областей компьютера:

- **Проверка объектов автозапуска** - проверка всех запускаемых файлов во время загрузки операционной системы **Windows**. По умолчанию расписание включено на режим **После запуска приложения**. Нажмите кнопку **Изменить** напротив этой опции для того, чтобы задать необходимое расписание.

- **Проверка критических областей** - проверка системных файлов, объектов автозапуска, системной памяти, загрузочных секторов дисков, системной памяти. По умолчанию расписание не включено. Нажмите кнопку **Изменить** напротив этой опции для того, чтобы задать необходимое расписание.

- **Полная проверка компьютера** - проверка всех файлов компьютера, а также критических областей на вирусы. По умолчанию расписание не включено. Нажмите кнопку **Изменить** напротив этой опции для того, чтобы задать необходимое расписание.



Задайте необходимые настройки для системных задач проверки **Объектов автозапуска, Критических областей и Моего компьютера** и нажмите кнопку Далее для продолжения первоначальной настройки антивируса Касперского версии 6.0

**2 способ.**В антивирусе Касперского версии 6.0 системные задачи удалить нельзя. Их можно только остановить, запустить или приостановить

- **Критические области** - проверка на присутствие вирусов всех критических областей компьютера. К ним относятся: системная память, объекты, исполняемые при старте системы, загрузочные сектора дисков, системные каталоги ***Windows*** и ***system32.*** Цель задачи - быстрое обнаружение в системе активных вирусов, без запуска полной проверки компьютера.

- **Мой Компьютер** - поиск вирусов на вашем компьютере с тщательной проверкой всех подключенных дисков, памяти, файлов.

- **Объекты автозапуска** - проверка на присутствие вирусов объектов, загрузка которых осуществляется при старте операционной системы.

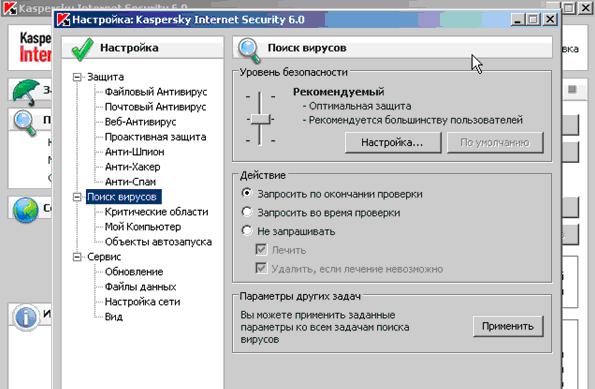
Настройки можно задать как для каждой задачи отдельно, так и для всех задач вместе.

Для того, чтобы задать настройки для всех задач вместе, необходимо сделать следующее:

- Откройте главное окно антивируса Касперского версии 6.0

- Выберите раздел **Поиск Вирусов**

- Нажмите кнопку **Настройка**



В главном окне настроек можно изменить следующие параметры:

- **Уровень безопасности** - выбрать один из трех уровней безопасности, установить пользовательский уровень безопасности, установить уровень безопасности по умолчанию

- **Действие над объектом** - запросить по окончании проверки, запросить во время проверки или не запрашивать, а лечить или удалить, если лечение невозможно.

- **Параметры других задач** - применить заданные параметры для **Поиска Вирусов** к трем системным задачам **Критические области, Мой Компьютер, Объекты автозапуска**, а также к пользовательским задачам, если они были созданы ранее.

**Настройка проактивной защиты**

В процессе установки **Антивируса Касперского 6.0 MP1\6.0 MP2, Kaspersky Internet Security 6.0 MP1\6.0 MP2 и Антивируса Касперского 6.0 для Windows Workstations MP2\MP3** Мастер первоначальной настройки предлагает настроить компонент **Проактивная защита:**

**Базовая защита** - включены модули Анализ активности приложений и проверка VBA-макросов. Для Анализа активности включены функции:

- опасная активность (анализ поведения приложения в системе)

- внедрение в процесс (invaders)

- появления скрытого процесса (rootkit)

- подозрительные значения в реестре

- подозрительная активность в системе

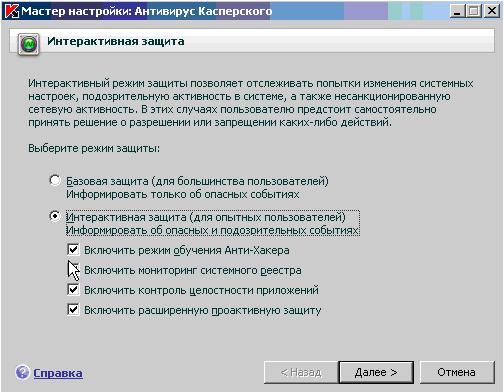
- обнаружение клавиатурных перехватчиков

**Интерактивная защита** - расширенные модули включаются по желанию пользователя, а именно:

- Режим обучения Анти-хакера. По умолчанию Анти-хакер работает в режиме Минимальная защита. В режиме Минимальная Защита Анти-хакер использует предустановленные правила для приложений и пакетов, созданные специалистами Лаборатории Касперского на основе многолетнего опыта работы. В режиме обучения Анти-хакер позволяет пользователю самостоятельно разрешать или запрещать доступ приложеням, устанавливающим соедининение с Интернет.

- Мониторинг системного реестра позволяет контролировать пользователю любое изменение в системном реестре операционной системы Windows.

- Контроль целостности приложений отслеживает попытки загрузки модулей в контролируемые приложения



**Расширенная проактивная защита** включает для модуля Анализ активности приложений дополнительные функции:

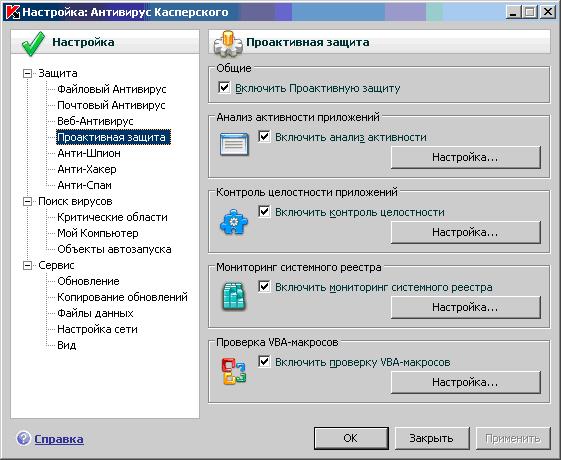
- запуск браузера с параметрами

- внедрение оконных перехватчиков.

Выберите необходимый тип защиты для компонента **Проактивная защита** и нажмите кнопку **Далее** для продолжения первоначальной настройки антивируса Касперского версии 6.0

С каждым днем вредоносных программ становится все больше, они усложняются, комбинируя в себе несколько видов, методы распространения становятся все более сложными для обнаружения.

Для того чтобы обнаружить новую вредоносную программу еще до того, как она успеет нанести вред, специалистами **Лабораторией Касперского** разработан специальный компонент - **Проактивная защита.** Он основан на контроле и анализе поведения всех программ, установленных на вашем компьютере. На основании выполняемых действий Антивирус Касперского версии 6.0 принимает решение: является программа опасной или нет. Таким образом, Ваш компьютер защищен не только от уже известных вирусов, но и от новых, еще не исследованных.



Возможности компонента **Проактивная защита:**

**анализ активности приложений:** осуществляет контроль:

- опасная активность процессов

- запуск браузера с параметрами

- внедрение в процесс**(invaders)**

- появление скрытого процесса **(rootkit)** в системе

- внедрения оконного перехватчика

- подозрительные значения в реестре

- подозрительная активность в системе

- обнаружение клавиатурных перехватчиков

- защита **Диспетчера задач Windows**



**Контроль Опасной активности:** анализирует поведение всех процессов, запущенных в системе, сохраняя все изменения, производимые в файловой системе и реестре. При выполнении некоторым приложением набора подозрительных действий выдаётся предупреждение пользователю об опасности данного процесса.

**Откат изменений после определения опасной активности в системе:** технология, позволяющая восстанавливать систему после вредоносных действий, возвращая ее к незараженному состоянию.

**Контроль запуска браузера с параметрами:** позволяет перехватить скрытый запуск браузера с передачей ему параметров, что может быть использовано вредоносными программами.

**Контроль внедрения кода в чужые процессы:** позволяет перехватить все возможности внедрения программного кода в чужие процессы.

**Технология борьбы с руткитами (контроль появления скрытого процесса):** позволяет обнаруживать большинство из реализаций современных руткитов, которые могут скрывать от пользователя файлы, папки и ключи реестра, скрывать запущенные программы, системные службы, драйверы и сетевые соединения, скрывать сетевую активность.

**Контроль внедрения оконного перехватчика:** перехватывает попытку внедрения динамической библиотеки во все активные процессы в системе.

**Подозрительные значения в реестре:** позволяет перехватить попытку создания «скрытых» ключей в реестре, не отображаемых обычными программами (типа regedit).

**Подозрительная активность в системе:** отслеживает большое число различных изменений в системе, указывающих на присутствие активного вредоносного кода.

**Обнаружение клавиатурных перехватчиков:** отслеживает перехваты вредоносными программами информации, вводимой с клавиатуры.

**Защита Диспетчера задач Microsoft Windows:** позволяет защитить **Диспетчер задач** от внедрения вредоносных модулей, деятельность которых направлена на блокирование работы **Диспетчера.**

**Контроль целостности приложений (монитор приложений):** позволяет задавать ряд приложений, для которых будет контролироваться компонентный состав.

**Контроль системного реестра (монитор реестра):** контролирует изменения ключей реестра. Содержит предустановленный список из 6 групп критических ключей. Также пользователь может добавить свои группы ключей и настроить правила доступа к ним для различных приложений.

**Проверка VBA-макросов:** Проверка опасных макросов Visual Basic for Application.

**Настройка компонента Файловый антивирус**

**Файловый Антивирус** - компонент, контролирующий файловую систему компьютера. Он проверяет все ОТКРЫВАЕМЫЕ, ЗАПУСКАЕМЫЕ И СОХРАНЯЕМЫЕ файлы на вашем компьютере и всех присоединенных по сети дисках. Каждый файл, к которому вы обратитесь, будет перехвачен Антивирусом Касперского и проверен на присутствие известных вирусов. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен Антивирусом Касперского. Если же файл по каким-либо причинам невозможно вылечить, он будет удален или помещен на карантин.

Для того, чтобы посмотреть и\или изменить настройки **Файлового Антивируса**, необходимо сделать следующее:

- Откройте главное окно антивируса Касперского версии 6.0

- Нажмите кнопку **Настройка**

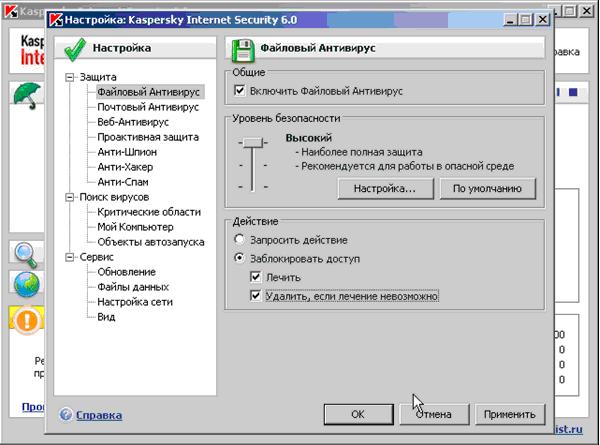
- В левой части диалогового окна в разделе Защита выберите пункт меню Файловый Антивирус

Для компонента **Файловый Антивирус** предусмотрены следующие настройки:

- Включить **Файловый Антивирус** - включить или отключить работу компонента **Файловый Антивирус.**

- **Уровень безопасности** - выбрать один из трех уровней безопасности, установить пользовательский уровень безопасности, установить уровень безопасности по умолчанию

- **Действие над объектом** - запросить по окончании проверки, запросить во время проверки или не запрашивать, а лечить или удалить, если лечение невозможно.



**Уровни безопасности Файлового антивируса**

**Высокий** - уровень, на котором осуществляется максимально полный контроль за открываемыми, сохраняемыми и запускаемыми файлами. Для этого уровня заданы следующие параметры:

- Проверять все файлы

- Проверять все архивы

- Проверять все инсталляционные пакеты

- Проверять только новые вложенные OLE-объекты

- Режим проверки - интеллектуальный

**Рекомендуемый** - уровень, параметры которого рекомендованы экспертами **Лаборатории Касперского**. Для этого уровня заданы следующие параметры:

- Проверять программы и документы по содержимому

- Проверять только новые и измененные файлы

- Проверять вложенные OLE-объекты

- Не распаковывать файл, если его размер больше 8 МБ

- Режим проверки - интеллектуальный

**Низкий** - уровень с параметрами, которые позволяют вам комфортно работать с приложениями, требующими значительных ресурсов оперативной памяти, поскольку набор проверяемых файлов на данном уровне сокращен. Для этого уровня заданы следующие параметры:

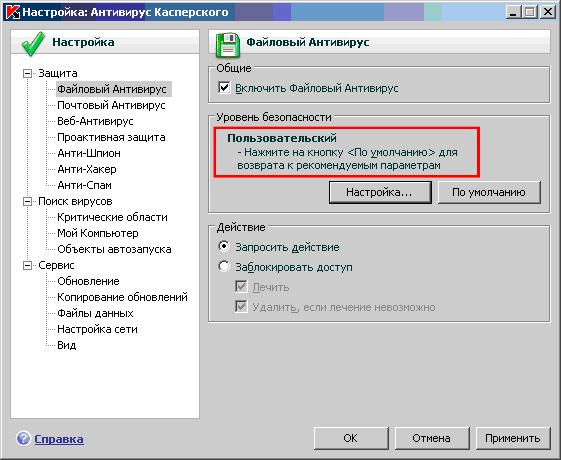
- Проверять программы и документы по содержимому

- Проверять только новые и измененные файлы

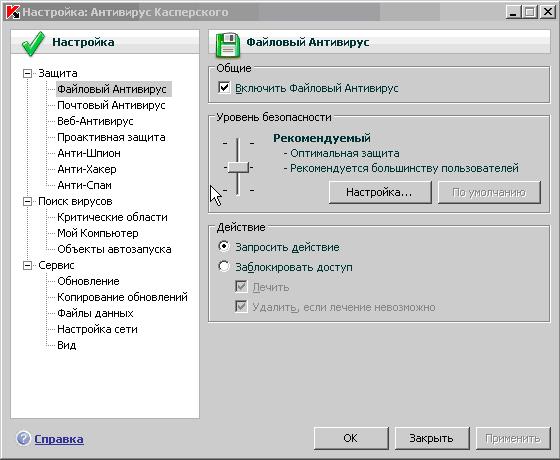
- Не распаковывать файл, если его размер больше 8 МБ

- Режим проверки - интеллектуальный

**Пользовательски**й - уровень, настройки которого не соответсвуют ни одному уровню из перечисленных выше. После того, как Вы изменили вручную настройки одного из выше перечисленных уровней и сохранили их, вновь созданному(измененному) уровню присвается название **Пользовательский.**

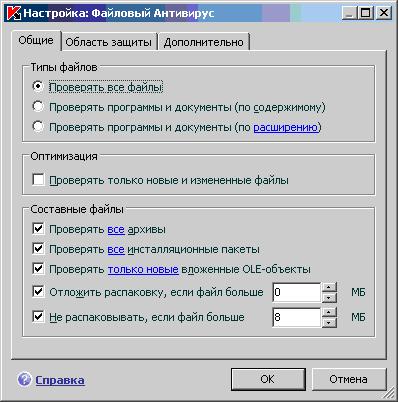


Для перехода в меню настроек нажмите кнопку **Настройка** в разделе Уровни безопасности окна **Настроек**



Для любого из трех уровней можно изменить следующие настройки:

**Закладка Общие:**



- **Проверять все файлы** - в данном случае проверке будут подвергаться все без исключения объекты

- **Проверять программы и документы (по содержимому)** - при выборе такой группы программа будет проверять только потенциально заражаемые объекты - файлы, в которые может внедриться вирус. Прежде чем приступать к поиску вирусов в объекте, выполняется анализ его внутреннего заголовка на предмет формата файла (txt, doc, exe и т.д.)

- **Проверять программы и документы (по расширению)** - в этом случае программа будет проверять только потенциально заражаемые файлы, при этом формат файла будет определяться на основании его расширения. Воспользовавшись ссылкой расширению, Вы можете ознакомиться со списком расширений файлов, которые подвергаются проверке в данном случае

- Проверять только новые и измененные файлы - в этом случае программа проверит новый файл один раз. Если файл не будет изменяться, то он не будет проверен.

- **Проверять *Все\Только* *новые* архивы** - проверка архивов **RAR, ARJ, ZIP, CAB, LHA, JAR, ICE**

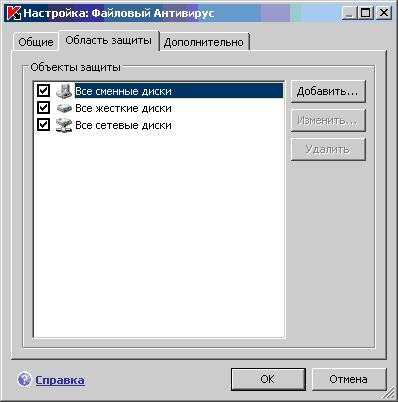
- **Проверять *Все\Только* *новые* инсталляционные пакеты** - проверка на вирусы самораспаковывающихся архивов

- **Проверять *Все\Только новые* вложенные OLE-объекты** - проверка погруженных в файл объектов (например, Excel-таблица или макрос)

- **Отложить распаковку, если файл больше** - в случае, если размер составного объекта превышает данное ограничение, он будет проверен программой как единый объект (проанализирован заголовок) и предоставлен пользователю для работы. Проверка объектов, входящих в его состав, будет произведена позже. Если флажок не установлен, доступ к файлам больше указанного размера блокируется до завершения проверки объектов

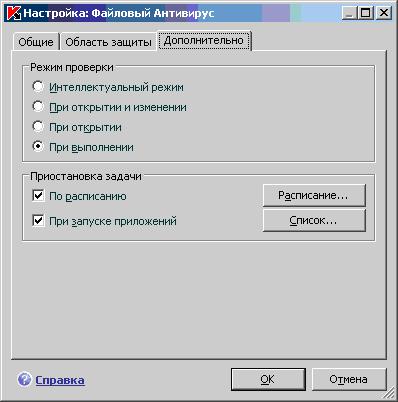
- **Не распаковывать, если файл больше** - в этом случае файл больше указанного размера будет пропущен без антивирусной проверки

**Закладка Область защиты:**



На этой закладке Вы можете добавить, изменить или удалить область защиты для компонента **Файловый Антивирус**. По умолчанию в режиме постоянной защиты проверяются файлы на всех жестких, сменных и подключенных по сети дисках Вашего компьютера.

Закладка **Дополнительно:**



На закладке **Дополнительно** Вы можете изменить режим работы компонента **Файловый Антивирус:**

- **Интеллектуальный режим** - данный режим направлен на повышение скорости обработки объектов и предоставления их пользователю для работы. При его выборе решение о проверке принимается на основании анализа операций, выполняемых с объектом. Например, при работе с документом **Microsoft Office** антивирус Касперского версии 6.0 проверяет файл при первом открытии и последнем закрытии. Все промежуточные операции перезаписи файла из проверки исключаются.

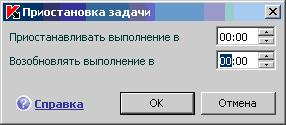
- **При открытии и изменении** - проверять объекты компонентом **Файловый Антивирус** при открытии и изменении объекта.

- **При открытии** - проверять объекты только при попытке открытия.

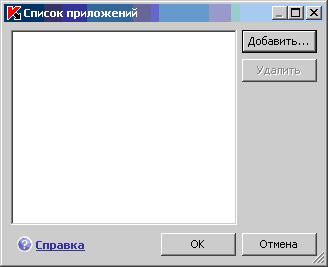
- **При выполнении -** проверять объекты только в момент попытки запуска.

Также на закладке **Дополнительно** Вы можете задать расписание приостановки работы компонента **Файловый Антивирус:**

- **По расписанию** - приостановка и запуск компонента **Файловый Антивирус.** Нажмите кнопку **Расписание** для того, чтобы установить время приостановки и время возобновления работы компонента **Файловый Антивирус.**



- **При запуске приложений** - приостановка и запуск компонента **Файловый Антивирус** будет осуществляться при запуске заданного Вами приложения и его закрытии соответственно. Нажмите кнопку **Список** для того, чтобы добавить приложения или удалить их.



**Настройка компонента Почтовый Антивирус**

В состав антивируса Касперского версии 6.0 входит специальный компонент, обеспечивающий защиту входящей и исходящей почты на наличие опасных объектов, - **Почтовый Антивирус**. Компонент по умолчанию запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все почтовые сообщения протоколов **POP3, SMTP, IMAP, MAPI и NNTP.**

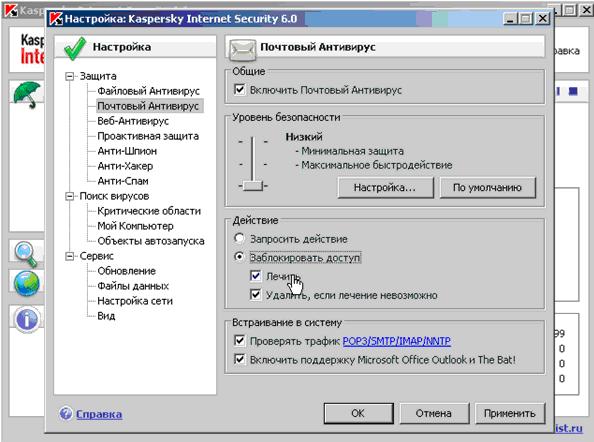
*Почтовый трафик по протоколу MAPI проверяется только плагинами Microsoft Office Outlook и The Bat!*

Для того, чтобы перейти в окно настроек компонента **Почтовый Антивирус**, необходимо сделать следующее:

- Откройте главное окно антивируса Касперского версии 6.0

- Нажмите кнопку **Настройка**

- В левой части диалогового окна в разделе **Защита** выберите пункт меню **Почтовый Антивирус**



Для компонента **Почтовый Антивирус** предусмотрены следующие настройки:

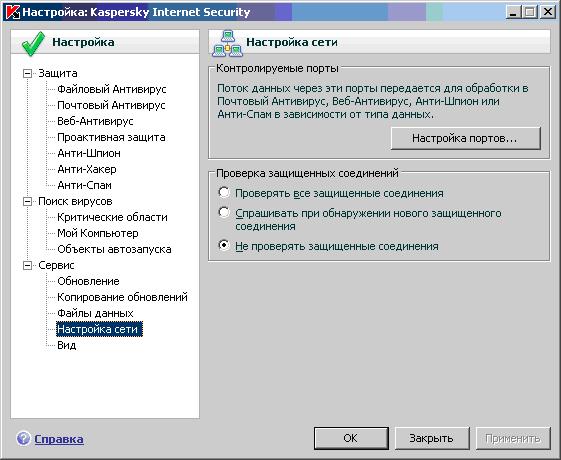
- **Включить Почтовый Антивирус** - включить или отключить работу компонента **Почтовый Антивирус.**

- **Уровень безопасности** - выбрать один из трех уровней безопасности, установить пользовательский уровень безопасности, установить уровень безопасности по умолчанию

- **Действие над объектом** - запросить по окончании проверки, запросить во время проверки или не запрашивать, а лечить или удалить, если лечение невозможно

- **Проверять трафик *POP3/SMTP/IMAP/NNTP*** - проверять почтовый трафик по по протоколам **POP3, SMTP, IMAP и NNTP.** Воспользовавшись ссылкой ***POP3/SMTP/IMAP/NNTP*** Вы можете отредактировать список контролируемых портов, а также включить\отключить проверку защищенных (SSL) соединений.

Опция проверки защищенных **(SSL)** соединений недоступна в **Антивирусе Касперского 6.0 и Kaspersky internet Security 6.0**



- **Включить поддержку Microsoft Office Outlook и The Bat! -** включить\отключить проверку почтового трафика для почтовых клиентов **Microsoft Office Outlook и The Bat!**

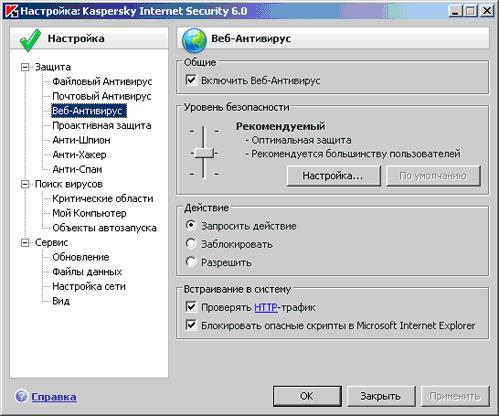
Если Вы отключаете все опции из блока **Встраивание в систему,** а именно опцию **Проверять трафик *POP3/SMTP/IMAP/NNTP***и опцию **Включить поддержку Microsoft Office Outlook и The Bat!,** то компонент **Почтовый Антивирус** автоматически выключается, а настройки становятся не доступными для изменения. В этом случае не имеет смысла использовать компонент **Почтовый Антивирус**, так как все области защиты для этого компонента были отключены.

**Настройка компонента Веб-антивирус**

Компонент **Веб-антивирус,** входящий в состав продуктов **Лаборатории Касперского версии 6.0\7.0,** выполняет две функции:

- осуществляет антивирусную проверку трафика, передающегося по протоколу **HTTP**. Таким образом, осуществляется защита любого интернет браузера, в том числе **Mozilla Firefox** и **Opera.**

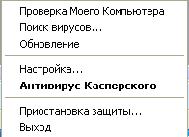
- обеспечивает контроль над всеми запускающимися скриптами на **Java-script** и **VB-script.** Осуществлением данного контроля занимается усовершенствованная версия **Kaspersky Script checker.**



**Работа антивируса**

Когда происходит важное с точки зрения антивирусной безопасности событие, на некоторое время над значком появляется информационное сообщение с рекомендацией от экспертов Лаборатории Касперского.

Если вы нажмете правой клавишей мыши в системной панели по значку приложения, откроется контекстное меню, состоящее из следующих пунктов:



Главное окно Антивируса Касперского предназначено для реализации всех возможностей приложения по обеспечению полной антивирусной защиты вашего компьютера. Здесь вы можете:

- запускать задачи антивирусной защиты;

- загружать обновления антивирусных баз;

- работать с объектами, находящимися на карантине и в резервном хранилище;

- работать с отчетами и т.д.

Все параметры антивирусной защиты, необходимая информация и задачи сгруппированы в главном окне на следующих закладках:

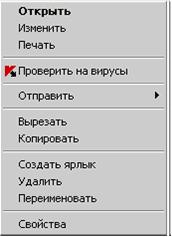
- **Защита** - статус и задачи антивирусной защиты. Данная закладка является основной при работе с приложением.

- **Сервис** - информация, необходимая в случае возникновения проблем или необходимости обращения за помощью в Лабораторию Касперского; возможность настройки точек обновления антивирусной программы.

- **Поиск вирусов** - предоставляет возможность выбора необходимых объектов для проверки.

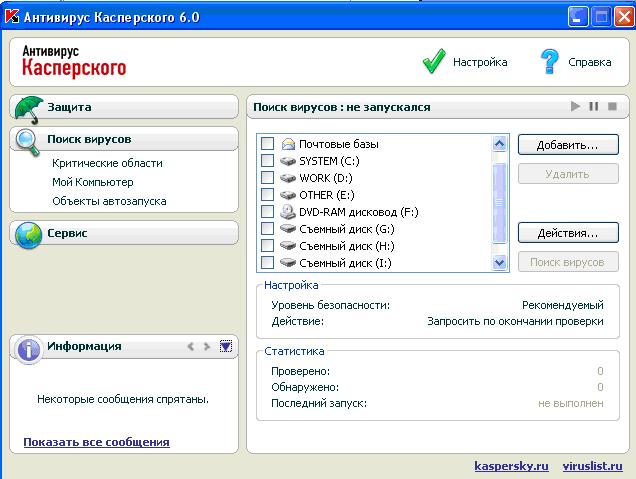
Бывают ситуации, когда необходимо проверить на присутствие вирусов не весь компьютер, а отдельный объект, например, один из жестких дисков, на котором находятся программы и игры, почтовые базы, принесенные с работы, пришедший по почте архив и т.п. Выбрать объект для проверки вы можете как при помощи Антивируса Касперского, так и стандартными средствами операционной системы Windows (например, в окне программы **Проводник** или на **Рабочем столе** и т.д.).

- Чтобы запустить проверку объекта, выбранного средствами Windows, установите курсор мыши на имени выбранного объекта, по правой кнопке мыши откройте контекстное меню Windows и выберите пункт **Проверить на.**



Проверка на присутствие вирусов объекта, выбранного средствами Windows

Для того чтобы запустить антивирусную проверку съемного диска или отдельного объекта, выберите в левой части закладки **Поиск вирусо**в и выбрать объекты для проверки.



Чтобы проверить некоторые объекты списка,

1. Установите флажки слева от объектов списка, которые необходимо проверить.

2. Нажмите на кнопку **Поиск вирусов** для запуска проверки. Независимо от того, каким способом была запущена проверка объекта (из контекстного меню Windows или из списка объектов Антивируса Касперского), на экране откроется окно Проверка, где будет отображаться процентное выполнение задания, информация о времени начала проверки, планируемого или реального времени окончания проверки, а также имя проверяемого объекта.

**Задание**

1. Настройте обновление сигнатур антивирусной программы и обновите их.

2. Изучите настройки Файлового, Почтового и Веб - антивируса.

3. Проверьте любой внешний носитель информации на вирусы.

4. Сохраните файл отчета о проверке носителя и с настройками антивируса в виде текстового документа. Результат покажите преподавателю.

**Контрольные вопросы:**

1. Что такое антивирусная программа?
2. Какие антивирусные программы вам известны?
3. Какие классы вирусов и потенциально опасных программ вы знаете?
4. Какой вид может принять значок антивируса Касперского в системной панели?
5. Что такое проактивная защита? Как ее настроить?
6. Какие уровни защиты предлагает проактивная защита?
7. Что такое файловый антивирус?
8. Назовите уровни безопасности файлового антивируса.
9. Назовите режимы проверки файлового антивируса.
10. Какие функции выполняет почтовый антивирус?
11. Какие закладки находятся в главном окне антивируса, что они содержат и для чего они предназначены?
12. Как выбрать объект для проверки на присутствие вирусов?

# Лабораторная работа 9 Восстановление зараженных файлов. Профилактика проникновения «троянских программ»

**Цель занятия:** Ознакомиться с основными возможностями «системного реестра» операционной системы **Windows 7** по настройке параметров безопасности.

Изучить последовательность операций по проверке потенциальных мест размещения вирусов в ОС **Windows 7**

Приобрести практические навыки по защите компьютера от несанкционированных действий «троянских программ».

**Норма времени**: 2 часа

**Методическое обеспечение:** методические указания к практической работе

**Теоретические сведения**

Реестр операционных систем Windows

Реестр – это большая база данных, где хранится информация о конфигурации системы. Этой информацией пользуются как Windows, так и другими программами.

В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работоспособную версию реестра, но для этого, естественно, необходимо иметь копию реестра.

Основным средством для просмотра и редактирования записей реестра служит специализированная утилита «Редактор реестра».

Файл редактора реестра находится в папке Windows. Называется он regedit.exe. После запуска появится окно редактора реестра. Вы увидите список из 5 разделов (Рисунок 1):

HKEY\_CLASSES\_ROOT

HKEY\_CURRENT\_USER

HKEY\_LOCAL\_MACHINE

HKEY\_USERS

HKEY\_CURRENT\_CONFIG

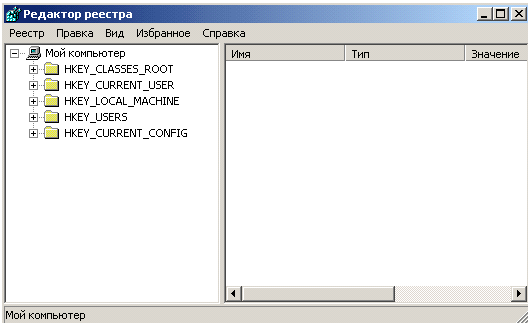


Рисунок 1

Работа с разделами реестра аналогична работе с папками в Проводнике. Конечным элементом дерева реестра являются ключи или параметры, делящиеся на три типа (Рисунок 2):

строковые (напр. "C:\Windows");

двоичные (напр. 10 82 A0 8F);

DWORD - этот тип ключа занимает 4 байта и отображается в шестнадцатеричном и в десятичном виде (например, 0x00000020 (32)).

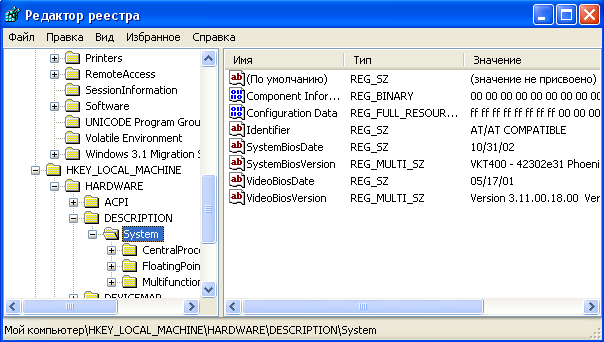


Рисунок 2

В Windows системная информация разбита на так называемые ульи (hive). Это обусловлено принципиальным отличием концепции безопасности этих операционных систем. Имена файлов ульев и пути к каталогам, в которых они хранятся, расположены в разделе **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist** (Рисунок 3).

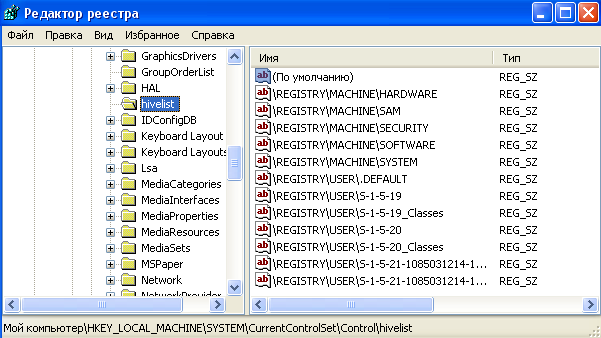


Рисунок 3

В таблице даны краткие описания ульев реестра и файлов, в которых хранятся параметры безопасности.

Таблица 1

|  |  |
| --- | --- |
| **HKEY\_LOCAL\_MACHINE \SAM** | Содержит информацию SAM (Security Access Manager), хранящуюся в файлах SAM, SAM.LOG, SAM.SAV в папке \%Systemroot%\System32\Config. |
| **HKEY\_LOCAL\_MACHINE \SECURITY** | Содержит информацию безопасности в файлах SECURITY, SECURITY.LOG, SECURITY.SAV в папке \%Systemroot%\System32\Config. |
| **HKEY\_LOCAL\_MACHINE \SYSTEM** | Содержит информацию об аппаратных профилях этого подраздела. Информация хранится в файлах SYSTEM, SYSTEM.LOG, SYSTEM.SAV в папке \%Systemroot%\System32\Config. |
| **HKEY\_CURRENT\_CONFIG** | Содержит информацию о подразделе System этого улья, которая хранится в файлах SYSTEM.SAV и SYSTEM.ALT в папке \%Systemroot%\System32\Config. |
| **HKEY\_USERS\.DEFAULT** | Содержит информацию, которая будет использоваться для создания профиля нового пользователя, впервые регистрирующегося в системе. Информация хранится в файлах DEFAULT, DEFAULT.LOG, DEFAULT.SAV в папке \%Systemroot%\System32\Config. |
| **HKEY\_CURRENT\_USER** | Содержит информацию о пользователе, зарегистрированном в системе на текущий момент. Эта информация хранится в файлах NTUSER.DAT и NTUSER.DAT.LOG, расположенных в каталоге \%Systemroot%\Profiles\Username, где Username - имя пользователя, зарегистрированного в системе на данный момент. |

**Задание:**

Проверить потенциальные места записей «троянских программ» в системном реестре.

**Алгоритм выполнения работы**

Потенциальными местами записей «троянских программ» в системном реестре являются разделы, описывающие программы, запускаемые автоматически при загрузке операционной системы от имени пользователей и системы.

**Для этого выполните следующие действия.**

Запустите программу **regedit.exe**.

В открывшемся окне выберите ветвь **HKEY\_LOCAL\_MACHINE** и далее

**Software\Microsoft\WindowsNT\CurrentVersion\Winlogon.**

В правой половине открытого окна программы **regedit.exe** появится список ключей.

Найдите ключ **Userinit (REG\_SZ)** и проверьте его содержимое.

По умолчанию (исходное состояние) – этот ключ содержит следующую запись **C:\WINDOWS\system32\userinit.exe** (Рисунок 4).

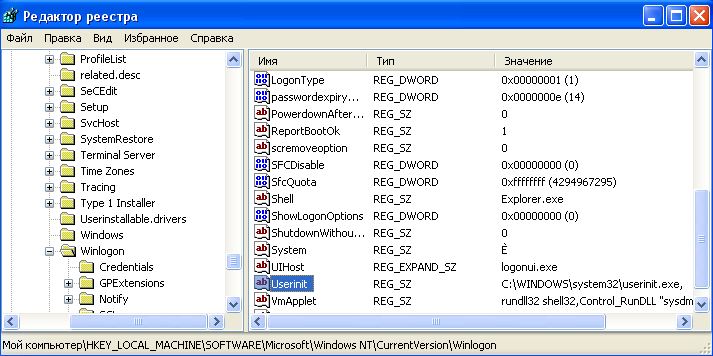


Рисунок 4

Если в указанном ключе содержатся дополнительные записи, то это могут быть троянские программы.

В этом случае проанализируйте место расположения программы, при этом обратите внимание на время создания файла и сопоставьте с Вашими действиями в это время.

Если время создания файла совпадает с временем Вашей работы в Интернете, то возможно, что в это время Ваш компьютер был заражен троянским конем.

Для удаления этой записи необходимо дважды щелкнуть на названии ключа (или при выделенном ключе выбрать команду **Изменить** из меню **Правка** программы **regedit.exe**).

В открывшемся окне в поле **Значение** (Рисунок 5) удалите ссылку на подозрительный файл.

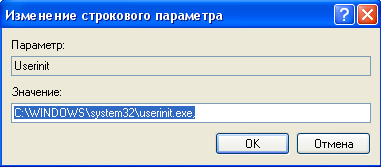


Рисунок 5

Закройте программу **regedit.exe.**

Перейдите в папку с подозрительным файлом и удалите его.

Перезагрузите операционную систему и выполните пункты задания 1-4.

Если содержимое, рассматриваемого ключа не изменилось, то предполагаемый «троянский конь» удален из Вашей системы.

Еще одним потенциальным местом записей на запуск «троянских программ» является раздел автозапуска **Run.**

Для его проверки выполните следующее.

Запустите программу **regedit.exe**.

В открывшемся окне выберите ветвь **HKEY\_LOCAL\_MACHINE и далее Software\Microsoft\Windows\CurrentVersion\Run\... (REG\_SZ)** (Рисунок 6).

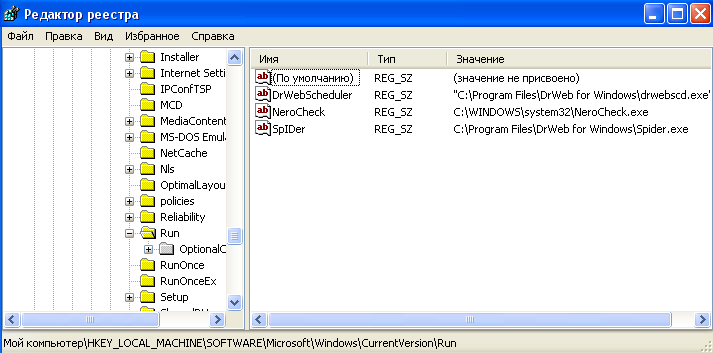


Рисунок 6 – Проверка содержимого раздела Run

В рассматриваемом примере автоматически запускается резидентный антивирус и его планировщик заданий, а также утилита, относящаяся к программе Nero (запись на CD).

Если в указанном разделе есть записи вызывающие подозрения, то выполните пункты 6-14 предыдущего задания.

**Задания для самостоятельной работы**

Проверьте содержимое ключа **HKEY\_LOCAL\_MACHINE \Software\Microsoft\WindowsNT\ CurrentVersion\Winlogon\System (REG\_SZ).**

Зафиксируйте этапы работы, используя команду PrintScreen клавиатуры.

Составьте отчет о результатах проверки.

**Контрольные вопросы**

Что такое реестр?

Поясните особенности «троянских программ».

Почему профилактика «троянских программ» связана с системным реестром?

Какие разделы и ключи являются потенциальными местами записей «троянских программ»?

# Список рекомендуемой литературы

**Основные источники**

1. Анин, Б. Ю. Защита компьютерной информации / Б.Ю. Анин. — СПб.: БХВ-Санкт-Петербург, 2010. – 384 с.
2. Касперски, К. Записки исследователя компьютерных вирусов / К. Касперски. – СПб.: Питер, 2006. – 316 с.
3. Корнюшин, П.Н. Информационная безопасность / П.Н. Корнюшин, С.С. Костерин. – Владивосток: Изд-во ДвГУ, 2010. – 154 с.
4. Партыка Т.Л. Информационная безопасность / Т.Л. Партыка, И. И. Попов.— М.: ФОРУМ: ИНФРА-М, 2012. — 432 с.

**Дополнительные источники**

1. Аскеров, Т. М. Защита информации и информационная безопасность / Т.М. Аскеров. — М.: Издательство РЭА им. Плеханова, 2009. – 387 с.
2. Будко, В.Н. Информационная безопасность и защита информации. Конспект лекций / В.Н. Будко. – Воронеж: Издательство ВГУ, 2010. – 86 с.
3. Сычев, Ю.Н. Основы информационной безопасности / Ю.Н. Сычев. – М.: Евразийский открытый институт, 2010. – 328 с.