**Практическая работа № 1. Обнаружение вируса и устранение последствий его влияния**

Цель работы: способы обнаружения вирусов и устранение последствий их вляяния Теоретический материал Классификация компьютерных вирусов В настоящее время в мире насчитывается более 40 тысяч только зарегистрированных компьютерных вирусов. Так как подавляющее большинство современных вредительских программ обладают способностью к саморазмножению, то часто их относят к компьютерным вирусам. Все компьютерные вирусы могут быть классифицированы по следующим признакам:

• по среде обитания;

• по способу заражения;

• по степени опасности деструктивных (вредительских) воздействий;

• по алгоритму функционирования. По среде обитания компьютерные вирусы делятся на:

• сетевые;

• файловые;

• загрузочные;

• комбинированные. Средой обитания сетевых вирусов являются элементы компьютерных сетей. Файловые вирусы размещаются в исполняемых файлах. Загрузочные вирусы находятся в загрузочных секторах (областях) внешних запоминающих устройств (boot-секторах). Иногда загрузочные вирусы называют бутовыми. Комбинированные вирусы размещаются в нескольких средах обитания. Примером таких вирусов служат загрузочно-файловые вирусы. Эти вирусы могут размещаться как в загрузочных секторах накопителей на магнитных дисках, так и в теле загрузочных файлов. По способу заражения среды обитания компьютерные вирусы делятся на:

• резидентные;

• нерезидентные.

Резидентные вирусы после их активизации полностью или частично перемещаются из среды обитания (сеть, загрузочный сектор, файл) в оперативную память ЭВМ. Эти вирусы, используя, как правило, привилегированные режимы работы, разрешенные только операционной системе, заражают среду обитания и при выполнении определенных условий реализуют деструктивную функцию. В отличие от резидентных нерезидентные вирусы попадают в оперативную память ЭВМ только на время их активности, в течение которого выполняют деструктивную функцию и функцию заражения. Затем вирусы полностью покидают оперативную память, оставаясь в среде обитания. Если вирус помещает в оперативную память программу, которая не заражает среду обитания, то такой вирус считается нерезидентным. Арсенал деструктивных или вредительских возможностей компьютерных вирусов весьма обширен. Деструктивные возможности вирусов зависят от целей и квалификации их создателя, а также от особенностей компьютерных систем. По степени опасности для информационных ресурсов пользователя компьютерные вирусы можно разделить на:

• безвредные вирусы;

• опасные вирусы;

• очень опасные вирусы. Безвредные компьютерные вирусы создаются авторами, которые не ставят себе цели нанести какой-либо ущерб ресурсам КС. Ими, как правило, движет желание показать свои возможности программиста. Другими словами, создание компьютерных вирусов для таких людей - своеобразная попытка самоутверждения. Деструктивное воздействие таких вирусов сводится к выводу на экран монитора невинных текстов и картинок, исполнению музыкальных фрагментов и т. п. Однако при всей кажущейся безобидности таких вирусов они наносят определенный ущерб КС. Во-первых, такие вирусы расходуют ресурсы КС, в той или иной мере снижая ее 69 эффективность функционирования. Во-вторых, компьютерные вирусы могут содержать ошибки, вызывающие опасные последствия для информационных ресурсов КС. Кроме того, при модернизации операционной системы или аппаратных средств КС вирусы, созданные ранее, могут приводить к нарушениям штатного алгоритма работы системы. К опасным относятся вирусы, которые вызывают существенное снижение эффективности КС, но не приводящие к нарушению целостности и конфиденциальности информации, хранящейся в запоминающих устройствах. Последствия таких вирусов могут быть ликвидированы без особых затрат материальных и временных ресурсов. Примерами таких вирусов являются вирусы, занимающие память ЭВМ и каналы связи, но не блокирующие работу сети; вирусы, вызывающие необходимость повторного выполнения программ, перезагрузки операционной системы или повторной передачи данных по каналам связи и т. п. Очень опасными следует считать вирусы, вызывающие нарушение конфиденциальности, уничтожение, необратимую модификацию (в том числе и шифрование) информации, а также вирусы, блокирующие доступ к информации, приводящие к отказу аппаратных средств и наносящие ущерб здоровью пользователям. Такие вирусы стирают отдельные файлы, системные области памяти, форматируют диски, получают несанкционированный доступ к информации, шифруют данные и т. п. Известны публикации, в которых упоминаются вирусы, вызывающие неисправности аппаратных средств. Предполагается, что на резонансной частоте движущиеся части электромеханических устройств, например в системе позиционирования накопителя на магнитных дисках, могут быть разрушены. Именно такой режим и может быть создан с помощью программывируса. Другие авторы утверждают, что возможно задание режимов интенсивного использования отдельных электронных схем (например, больших интегральных схем), при которых наступает их перегрев и выход из строя. Использование в современных ПЭВМ постоянной памяти с возможностью перезаписи привело к появлению вирусов, изменяющих программы BIOS, что приводит к необходимости замены постоянных запоминающих устройств. Возможны также воздействия на психику человека - оператора ЭВМ с помощью подбора видеоизображения, выдаваемого на экран монитора с определенной частотой (каждый двадцать пятый кадр). Встроенные кадры этой видеоинформации воспринимаются человеком на подсознательном уровне. В результате такого воздействия возможно нанесение серьезного ущерба психике человека. В 1997 году 700 японцев попали в больницу с признаками эпилепсии после просмотра компьютерного мультфильма по телевидению. Предполагают, что именно таким образом была опробована возможность воздействия на человека с помощью встраивания 25-го кадра. В соответствии с особенностями алгоритма функционирования вирусы можно разделить на два класса

: • вирусы, не изменяющие среду обитания (файлы и секторы) при распространении;

• вирусы, изменяющие среду обитания при распространении. В свою очередь, вирусы, не изменяющие среду обитания, могут быть разделены на две группы:

• вирусы-"спутники" (соmраniоn);

• вирусы-"черви" (worm). Вирусы-"спутники" не изменяют файлы. Механизм их действия состоит в создании копий исполняемых файлов. Например, в MS-DOS такие вирусы создают копии для файлов, имеющих расширение .ЕХЕ. Копии присваивается то же имя, что и исполняемому файлу, но расширение изменяется на .СОМ. При запуске файла с общим именем операционная система первым загружает на выполнение файл с расширением .СОМ, который является программой-вирусом. Файл-вирус запускает затем и файл с расширением .ЕХЕ. Вирусы-"черви" попадают в рабочую станцию из сети, вычисляют адреса рассылки вируса по другим абонентам сети и осуществляют передачу вируса. Вирус не изменяет файлов и 70 не записывается в загрузочные секторы дисков. Некоторые вирусы-"черви" создают рабочие копии вируса на диске, другие - размещаются только в оперативной памяти ЭВМ. По сложности, степени совершенства и особенностям маскировки алгоритмов вирусы, изменяющие среду обитания, делятся на:

• студенческие;

• "стелс" - вирусы (вирусы-невидимки);

• полиморфные. К студенческим относят вирусы, создатели которых имеют низкую квалификацию. Такие вирусы, как правило, являются нерезидентными, часто содержат ошибки, довольно просто обнаруживаются и удаляются. "Стелc"-вирусы и полиморфные вирусы создаются квалифицированными специалистами, хорошо знающими принцип работы аппаратных средств и операционной системы, а также владеющими навыками работы с машиноориентированными системами программирования. "Стелс"-вирусы маскируют свое присутствие в среде обитания путем перехвата обращений операционной системы к пораженным файлам, секторам и переадресуют ОС к незараженным участкам информации. Вирус является резидентным, маскируется под программы ОС, может перемещаться в памяти. Такие вирусы активизируются при возникновении прерываний, выполняют определенные действия, в том числе и по маскировке, и только затем управление передается на программы ОС, обрабатывающие эти прерывания. "Стелс"-вирусы обладают способностью противодействовать резидентным антивирусным средствам. Полиморфные вирусы не имеют постоянных опознавательных групп - сигнатур. Обычные вирусы для распознавания факта заражения среды обитания размещают в зараженном объекте специальную опознавательную двоичную последовательность или последовательность символов (сигнатуру), которая однозначно идентифицирует зараженность файла или сектора. Сигнатуры используются на этапе распространения вирусов для того, чтобы избежать многократного заражения одних и тех же объектов, так как при многократном заражении объекта значительно возрастает вероятность обнаружения вируса. Для устранения демаскирующих признаков полиморфные вирусы используют шифрование тела вируса и модификацию программы шифрования. За счет такого преобразования полиморфные вирусы не имеют совпадений кодов. Любой вирус, независимо от принадлежности к определенным классам, должен иметь три функциональных блока: блок заражения (распространения), блок маскирования и блок выполнения деструктивных действий. Разделение на функциональные блоки означает, что к определенному блоку относятся команды программы вируса, выполняющие одну из трех функций, независимо от места нахождения команд в теле вируса. После передачи управления вирусу, как правило, выполняются определенные функции блока маскировки. Например, осуществляется расшифрование тела вируса. Затем вирус осуществляет функцию внедрения в незараженную среду обитания. Если вирусом должны выполняться деструктивные воздействия, то они выполняются либо безусловно, либо при выполнении определенных условий. Завершает работу вируса всегда блок маскирования. При этом выполняются, например, следующие действия: шифрование вируса (если функция шифрования реализована), восстановление старой даты изменения файла, восстановление атрибутов файла, корректировка таблиц ОС и др. Последней командой вируса выполняется команда перехода на выполнение зараженных файлов или на выполнение программ ОС. Для удобства работы с известными вирусами используются каталоги вирусов. В каталог помещаются следующие сведения о стандартных свойствах вируса: имя, длина, заражаемые файлы, место внедрения в файл, метод заражения, способ внедрения в ОП для резидентных вирусов, вызываемые эффекты, наличие (отсутствие) деструктивной функции и ошибки. Наличие каталогов позволяет при описании вирусов указывать только особые свойства, опуская стандартные свойства и действия. Известны следующие методы обнаружения вирусов:

• сканирование;

• обнаружение изменений;

• эвристический анализ;

• использование резидентных сторожей;

• вакцинирование программ;

• аппаратно-программная защита от вирусов. Сканирование - один из самых простых методов обнаружения вирусов. Сканирование осуществляется программой-сканером, которая просматривает файлы в поисках опознавательной части вируса - сигнатуры. Программа фиксирует наличие уже известных вирусов, за исключением полиморфных вирусов, которые применяют шифрование тела вируса, изменяя при этом каждый раз и сигнатуру. Программы-сканеры могут хранить не сигнатуры известных вирусов, а их контрольные суммы. Программы-сканеры часто могут удалять обнаруженные вирусы. Такие программы называются полифагами. Метод сканирования применим для обнаружения вирусов, сигнатуры которых уже выделены и являются постоянными. Для эффективного использования метода необходимо регулярное обновление сведений о новых вирусах. Самой известной программой-сканером в России является Aidstest Дмитрия Лозинского. Метод обнаружения изменений базируется на использовании программ-ревизоров. Эти программы определяют и запоминают характеристики всех областей на дисках, в которых обычно размещаются вирусы. При периодическом выполнении программ- ревизоров сравниваются хранящиеся характеристики и характеристики, получаемые при контроле областей дисков. По результатам ревизии программа выдает сведения о предположительном наличии вирусов. Обычно программы-ревизоры запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, характеристики всех контролируемых файлов, каталогов и номера дефектных кластеров. Могут контролироваться также объем установленной оперативной памяти, количество подключенных к компьютеру дисков и их параметры. Главным достоинством метода является возможность обнаружения вирусов всех типов, а также новых неизвестных вирусов. Совершенные программы-ревизоры обнаруживают даже "стелс"-вирусы. Например, программа-ревизор Аdinf, разработанная Д. Ю Мостовым, работает с диском непосредственно по секторам через Bios. Это не позволяет использовать "стелс"-вирусам возможность перехвата прерываний и "подставки" для контроля нужной вирусу области памяти. Имеются у этого метода и недостатки. С помощью программ-ревизоров невозможно определить вирус в файлах, которые поступают в систему уже зараженными. Вирусы будут обнаружены только после размножения в системе. Программы-ревизоры непригодны для обнаружения заражения макровирусами, так как документы и таблицы очень часто изменяются. Эвристический анализ сравнительно недавно начал использоваться для обнаружения вирусов. Как и метод обнаружения изменений, данный метод позволяет определять неизвестные вирусы, но не требует предварительного сбора, обработки и хранения информации о файловой системе. Сущность эвристического анализа заключается в проверке возможных сред обитания вирусов и выявление в них команд (групп команд), характерных для вирусов. Такими командами могут быть команды создания резидентных модулей в оперативной памяти, команды прямого обращения к дискам, минуя ОС. Эвристические анализаторы при обнаружении "подозри- 72 тельных" команд в файлах или загрузочных секторах выдают сообщение о возможном заражении. После получения таких сообщений необходимо тщательно проверить предположительно зараженные файлы и загрузочные сектора всеми имеющимися антивирусными средствами. Эвристический анализатор имеется, например, в антивирусной программе Doctor Web. Метод использования резидентных сторожей основан на применении программ, которые постоянно находятся в ОП ЭВМ и отслеживают все действия остальных программ. В случае выполнения какой-либо программой подозрительных действий (обращение для записи в загрузочные сектора, помещение в ОП резидентных модулей, попытки перехвата прерываний и т. п.) резидентный сторож выдает сообщение пользователю. Программа-сторож может загружать на выполнение другие антивирусные программы для проверки "подозрительных" программ, а также для контроля всех поступающих извне файлов (со сменных дисков, по сети). Существенным недостатком данного метода является значительный процент ложных тревог, что мешает работе пользователя, вызывает раздражение и желание отказаться от использования резидентных сторожей. Примером резидентного сторожа может служить программа Vsafe, входящая в состав MS DOS. Под вакцинацией программ понимается создание специального модуля для контроля ее целостности. В качестве характеристики целостности файла обычно используется контрольная сумма. При заражении вакцинированного файла, модуль контроля обнаруживает изменение контрольной суммы и сообщает об этом пользователю. Метод позволяет обнаруживать все вирусы, в том числе и незнакомые, за исключением "стеле"- вирусов. Самым надежным методом защиты от вирусов является использование аппаратно-программных антивирусных средств. В настоящее время для защиты ПЭВМ используются специальные контроллеры и их программное обеспечение. Контроллер устанавливается в разъем расширения и имеет доступ к общей шине. Это позволяет ему контролировать все обращения к дисковой системе. В программном обеспечении контроллера запоминаются области на дисках, изменение которых в обычных режимах работы не допускается. Таким образом, можно установить защиту на изменение главной загрузочной записи, загрузочных секторов, файлов конфигурации, исполняемых файлов и др. При выполнении запретных действий любой программой контроллер выдает соответствующее сообщение пользователю и блокирует работу ПЭВМ. Аппаратно-программные антивирусные средства обладают рядом достоинств перед программными:

• работают постоянно;

• обнаруживают все вирусы, независимо от механизма их действия;

• блокируют неразрешенные действия, являющиеся результатом работы вируса или неквалифицированного пользователя. Недостаток у этих средств один - зависимость от аппаратных средств ПЭВМ. Изменение последних ведет к необходимости замены контроллера. Примером аппаратно-программной защиты от вирусов может служить комплекс Sheriff. Ход работы Порядок действий пользователя при обнаружении заражения ЭВМ вирусами Даже при скрупулезном выполнении всех правил профилактики возможность заражения ЭВМ компьютерными вирусами полностью исключить нельзя. И если вирус все же попал в КС, то последствия его пребывания можно свести к минимуму, придерживаясь определенной последовательности действий. О наличии вируса в КС пользователь может судить по следующим событиям:

• появление сообщений антивирусных средств о заражении или о предполагаемом заражении;

• явные проявления присутствия вируса, такие как сообщения, выдаваемые на монитор или принтер, звуковые эффекты, уничтожение файлов и другие аналогичные действия, однозначно указывающие на наличие вируса в КС;

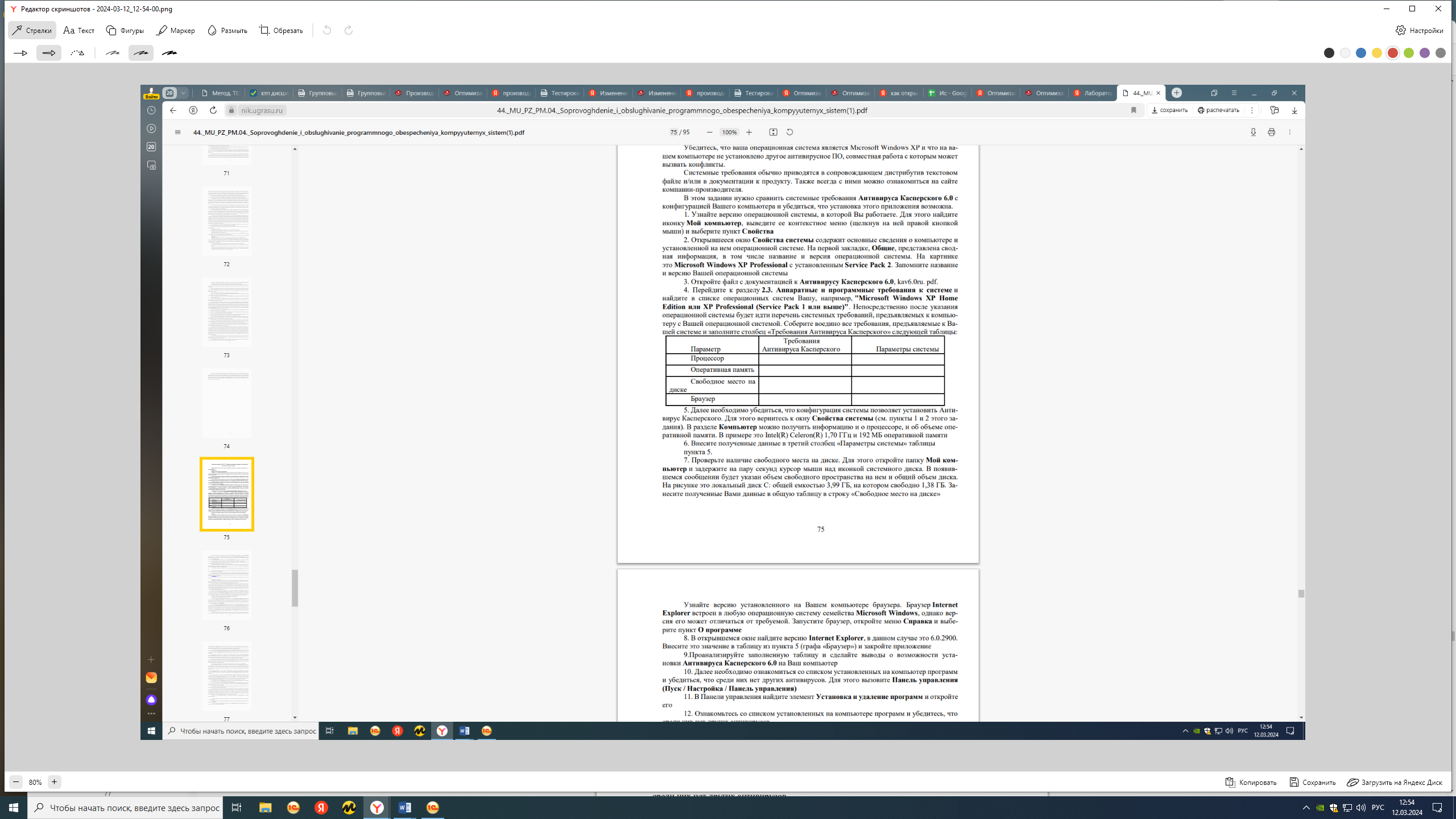
• неявные проявления заражения, которые могут быть вызваны и другими причинами, например, сбоями или отказами аппаратных и программных средств КС. К неявным проявлениям наличия вирусов в КС можно отнести "зависания" системы, замедление выполнения определенных действий, нарушение адресации, сбои устройств и тому подобное. Получив информацию о предполагаемом заражении, пользователь должен убедиться в этом. Решить такую задачу можно с помощью всего комплекса антивирусных средств. Убедившись в том, что заражение произошло, пользователю следует выполнить следующую последовательность шагов: Шаг 1. Выключить ЭВМ для уничтожения резидентных вирусов. Шаг 2. Осуществить загрузку эталонной операционной системы со сменного носителя информации, в которой отсутствуют вирусы. Шаг 3. Сохранить на сменных носителях информации важные для вас файлы, которые не имеют резервных копий. Шаг 4. Использовать антивирусные средства для удаления вирусов и восстановления файлов, областей памяти. Если работоспособность ЭВМ восстановлена, то осуществляется переход к шагу 8, иначе - к шагу 5. Шаг 5. Осуществить полное стирание и разметку (форматирование) несъемных внешних запоминающих устройств. В ПЭВМ для этого могут быть использованы программы MS-DOS FDISK и FORMAT. Программа форматирования FORMAT не удаляет главную загрузочную запись на жестком диске, в которой может находиться загрузочный вирус . Поэтому необходимо выполнить программу FDISK с недокументированным параметром MBR, создать с помощью этой же программы разделы и логические диски на жестком диске. Затем выполняется программа FORMAT для всех логических дисков. Шаг 6. Восстановить ОС, другие программные системы и файлы с дистрибутивов и резервных копий, созданных до заражения. Шаг 7. Тщательно проверить файлы, сохраненные после обнаружения заражения, и, при необходимости, удалить вирусы и восстановить файлы; Шаг 8. Завершить восстановление информации всесторонней проверкой ЭВМ с помощью всех имеющихся в распоряжении пользователя антивирусных средств. При выполнении рекомендаций по профилактике заражения компьютерными вирусами, а также при умелых и своевременных действиях в случае заражения .вирусами, ущерб информационным ресурсам КС может быть сведен к минимуму. В процессе удаления последствий заражения вирусами осуществляется удаление вирусов, а также восстановление файлов и областей памяти, в которых находился вирус. Существует два метода удаления последствий воздействия вирусов антивирусными программами. Первый метод предполагает восстановление системы после воздействия известных вирусов. Разработчик программы-фага, удаляющей вирус, должен знать структуру вируса и его характеристики размещения в среде обитания. Второй метод позволяет восстанавливать файлы и загрузочные сектора, зараженные неизвестными вирусами. Для восстановления файлов программа восстановления должна заблаговременно создать и хранить информацию о файлах, полученную в условиях отсутствия вирусов. Имея информацию о незараженном файле и используя сведения об общих принципах работы вирусов, осуществляется восстановление файлов. Если вирус подверг файл необратимым изменениям, то восстановление возможно только с использованием резервной копии или с дистрибутива. При их отсутствии существует только один выход - уничтожить файл и восстановить его вручную. Если антивирусная программа не может восстановить главную загрузочную запись или загрузочные сектора, то можно попытаться это сделать вручную. В случае неудачи следует отформатировать диск и установить ОС. Существуют вирусы, которые, попадая в ЭВМ, становятся частью его ОС. Если просто удалить такой вирус, то система становится неработоспособной. Одним из таких вирусов является вирус One Half. При загрузке ЭВМ вирус постепенно зашифровывает жесткий диск. При обращении к уже зашифрованным секторам резидентный вирус One Half перехватывает обращения и расшифровывает информацию. Удаление вируса приведет к невозможности использовать зашифрованную часть диска. При удалении такого вируса необходимо сначала расшифровать информацию на диске. Для этого необходимо знать механизм действия вируса.

**Практическая работа № 2. Установка и настройка антивируса. Настройка обновлений с помощью зеркала**

Цель работы: изучить системные требования антивируса, настройка обновлений с помощью зеркал

Ход работы

Задание 1. Системные требования Убедитесь, что ваша операционная система является Microsoft Windows XP и что на вашем компьютере не установлено другое антивирусное ПО, совместная работа с которым может вызвать конфликты. Системные требования обычно приводятся в сопровождающем дистрибутив текстовом файле и/или в документации к продукту. Также всегда с ними можно ознакомиться на сайте компании-производителя. В этом задании нужно сравнить системные требования Антивируса Касперского 6.0 с конфигурацией Вашего компьютера и убедиться, что установка этого приложения возможна. 1. Узнайте версию операционной системы, в которой Вы работаете. Для этого найдите иконку Мой компьютер, выведите ее контекстное меню (щелкнув на ней правой кнопкой мыши) и выберите пункт Свойства 2. Открывшееся окно Свойства системы содержит основные сведения о компьютере и установленной на нем операционной системе. На первой закладке, Общие, представлена сводная информация, в том числе название и версия операционной системы. На картинке это Microsoft Windows XP Professional с установленным Service Pack 2. Запомните название и версию Вашей операционной системы 3. Откройте файл с документацией к Антивирусу Касперского 6.0, kav6.0ru. pdf. 4. Перейдите к разделу 2.3. Аппаратные и программные требования к системе и найдите в списке операционных систем Вашу, например, "Microsoft Windows XP Home Edition или XP Professional (Service Pack 1 или выше)". Непосредственно после указания операционной системы будет идти перечень системных требований, предъявляемых к компьютеру с Вашей операционной системой. Соберите воедино все требования, предъявляемые к Вашей системе и заполните столбец «Требования Антивируса Касперского» следующей таблицы:



5. Далее необходимо убедиться, что конфигурация системы позволяет установить Антивирус Касперского. Для этого вернитесь к окну Свойства системы (см. пункты 1 и 2 этого задания). В разделе Компьютер можно получить информацию и о процессоре, и об объеме оперативной памяти. В примере это Intel(R) Celeron(R) 1,70 ГГц и 192 МБ оперативной памяти 6. Внесите полученные данные в третий столбец «Параметры системы» таблицы пункта 5. 7. Проверьте наличие свободного места на диске. Для этого откройте папку Мой компьютер и задержите на пару секунд курсор мыши над иконкой системного диска. В появившемся сообщении будет указан объем свободного пространства на нем и общий объем диска. На рисунке это локальный диск С: общей емкостью 3,99 ГБ, на котором свободно 1,38 ГБ. Занесите полученные Вами данные в общую таблицу в строку «Свободное место на диске»

Узнайте версию установленного на Вашем компьютере браузера. Браузер Internet Explorer встроен в любую операционную систему семейства Microsoft Windows, однако версия его может отличаться от требуемой. Запустите браузер, откройте меню Справка и выберите пункт О программе 8. В открывшемся окне найдите версию Internet Explorer, в данном случае это 6.0.2900. Внесите это значение в таблицу из пункта 5 (графа «Браузер») и закройте приложение 9.Проанализируйте заполненную таблицу и сделайте выводы о возможности установки Антивируса Касперского 6.0 на Ваш компьютер 10. Далее необходимо ознакомиться со списком установленных на компьютер программ и убедиться, что среди них нет других антивирусов. Для этого вызовите Панель управления (Пуск / Настройка / Панель управления) 11. В Панели управления найдите элемент Установка и удаление программ и откройте его 12. Ознакомьтесь со списком установленных на компьютере программ и убедитесь, что среди них нет других антивирусов 13. Обратите внимание на системную дату, установленную на Вашем компьютере. Для этого задержите на пару секунд курсор мышки над системным временем в правом нижнем углу экрана. Системная дата должна соответствовать реальной дате, это будет необходимо для корректной активации продукта На этом подготовительный этап окончен и можно переходить непосредственно к установке. Задание 2. Установка Стандартная процедура установки включает в себя копирование необходимых в работе программы файлов на диск (в нужное место) и регистрацию в реестре операционной системы. Иногда для завершения установки требуется перезагрузка компьютера. Для успешной установки Антивируса Касперского требуется дистрибутив и лицензионный ключ (файл с расширением. key, содержащий данные, удостоверяющие легальность приобретенного продукта). Эти файлы обычно записываются на CD и передаются пользователю при покупке. В случае приобретения в Интернет-магазине, дистрибутив можно либо загрузить с сайта Лаборатории Касперского, либо заказать отправку почтой или курьером на CD, лицензионный ключ высылается по e-mail. В этом задании необходимо произвести установку Антивируса Касперского 6.0. Для этого нужно запустить Мастер установки и проследовать за всеми его указаниями. По окончании установки запустится Мастер настройки. Он позволяет в режиме диалога с пользователем произвести настройку основных параметров работы антивируса. В большинстве случаев после этой процедуры дополнительная настройка по окончании инсталляции не требуется. 1.Откройте папку с дистрибутивом Антивируса Касперского. 2. Найдите файл setup. exe и запустите его 3. Если система удовлетворяет всем необходимым Антивирусу Касперского требованиям, запустится Мастер установки. В первом окне он поприветствует Вас и сообщит, что собирается сделать. Внимательно прочтите предложенный текст, выполните указание закрыть все сторонние открытые приложения (если таковые имеются) и нажмите кнопку Далее для перехода к следующему окну Мастера 4. На втором шаге Мастера необходимо ознакомиться с Лицензионным соглашением между Вами и Лабораторией Касперского, производителем Антивируса Касперского. В нем описаны все права и обязанности обоих сторон, в том числе ответственность за нарушение авторских прав и самостоятельное изготовление копий антивируса. Внимательно прочтите его. Установку можно продолжить только согласившись со всеми положениями, для этого нужно отметить пункт Я принимаю условия Лицензионного соглашения и нажать ставшую активной кнопку Далее 5. На следующем шаге нужно определить директорию, куда будут скопированы основные системные файлы антивируса. По умолчанию предлагается использовать C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0\. Если она по каким-то причинам не подходит, с помощью кнопки Обзор всегда можно выбрать другую. Для продолжения установки и перехода к следующему окну тут и в дальнейшем используйте кнопку Далее 6. Далее нужно выбрать тип установки: полную или выборочную. Полная означает установку всех компонентов Антивируса Касперского, а выборочная позволяет некоторые из них отключить. Выберите Выборочную, нажав на квадратную кнопку слева от описания этого типа установки 7. Как и было обещано, в следующем окне можно указать какие компоненты Антивируса Касперского необходимо установить, а какие пропустить. На рисунке изображен вид этого окна по умолчанию, соответствующий полной установке. Будет ли установлен тот или иной компонент символизирует иконка слева от него: - устанавливать, - нет Тут же можно получить краткое описание каждого компонента - для этого необходимо выделить (щелкнуть правой кнопкой мыши) интересующий компонент и внизу окна появится нужная информация. На рисунке выделен Антивирус Касперского 6.0, следовательно внизу показано описание самой программы. Оставьте установку всех компонентов и продолжите инсталляцию, нажав Далее 8.Далее Мастер проверяет наличие на компьютере других антивирусных программ, полный список которых можно найти в файле release\_notes. txt в разделе "Установка". Если такие найдутся, то пользователю будет выведено соответствующее уведомление с предложением их удалить. Но в нашем случае компьютер чист и этот этап в интерфейсе никак не отображается 9. На следующем этапе нужно подтвердить намерение установить программу, нажав Установить. После этого начнется непосредственное копирование файлов и регистрация программы в реестре, и вернуться к предыдущим окнам Мастера установки будет невозможно. Расположенный в центре окна флаг Включить защиту модулей до начала установки рекомендуется оставить включенным. Но в дальнейшем, при повторной инсталляции этой же версии Антивируса Касперского его следует очищать. Он отвечает за сохранность сделанных во время установки настроек, они могут потребоваться в дальнейшем для восстановления Антивируса Касперского в случае повреждения его программных модулей 10. Нажмите кнопку Установить и проследите за действиями Мастера. Они описываются непосредственно над индикатором процесса установки 11. По окончании инсталляции Мастер установки выводит информационное окно. Вам необходимо ознакомится с расположенным в нем текстом и запустить Мастер настройки приложения. Для этого нажмите Далее 12. На первом этапе настройки нужно активировать приложение. Это можно сделать одним из четырех предложенных вариантов: Используя код активации, коммерческий или пробный. Такой код может быть выдан при покупке через Интернет, в этом случае активация происходит также через Интернет Активировать используя полученный ранее ключевой файл - именно этот способ будет использован в этой лабораторной работе Активировать позже - если ключевого файла нет, то можно установить антивирус в пробном режиме, но в этом случае не будет доступно обновление антивирусных баз и следовательно, надежную защиту получить не получится Выберите вариант Использовать полученный ранее лицензионный ключ и нажмите Далее 13. В следующем окне нужно указать путь к лицензионному файлу. Для этого нажмите кнопку Обзор 14. Перейдите к указанной преподавателем папке с ключевым файлом, выделите его и нажмите Открыть 15. После открытия выбранного файла, в окне Мастера появится информация о нем. Ознакомьтесь с ней и нажмите Далее 16. На этапе перехода к следующему окну проводится проверка открытого лицензионного ключа. Если он действителен, то происходит его активация. Для продолжения настройки нажмите Далее 17. После активации начинается этап первоначальной настройки антивируса. Мастер установки предлагает настроить только основные параметры работы приложения и все сделанные в ходе инсталляции настройки впоследствии можно будет легко изменить с помощью графического интерфейса. Первое окно предлагает выбрать режим интерактивной защиты. Прочитайте описание различий между этими двумя режимами, оставьте выбранную по умолчанию Базовую защиту и нажмите Далее 18. Далее предлагается определить режим обновления, по умолчанию выбран пункт Автоматически. Он подходит для большинства пользователей. В этой лабораторной работе оставьте все настройки по умолчанию, поскольку задача обновления антивирусных баз будет подробно рассмотрена в одной из следующих лабораторных работ. Однако нужно знать, что в общем случае настроить и обновить антивирусные баз можно уже прямо в ходе установки (для этого предназначены кнопки Настройка и Обновить сейчас и меню выбора режима обновления) 19. В следующем окне можно задать настройки и расписание запуска проверки на наличие вирусов объектов автозапуска, критических областей и полной проверки компьютера. Для большинства пользователей рекомендуется настроить проверку объектов автозапуска (как наиболее часто поражаемой области компьютера) при каждой перезагрузке Антивируса Касперского. Это обычно соответствует каждой перезагрузке компьютера. Под проверкой критических областей подразумевается поиск вирусов в важных системных областях. По умолчанию это системная память, объекты автозапуска, загрузочные секторы дисков и папки C:\Windows и С:\Windows\system32. Полную проверку компьютера рекомендуется проводить раз в неделю. Однако поскольку она требует несколько больше системных ресурсов и соответственно может снижать общую производительность компьютера, оптимального расписания для всех пользователей нет. Поэтому если при установке на домашний компьютер Вы заранее знаете, что в определенный день и час полная проверка не будет мешать Вашей работе, то можете смело отмечать флаг Каждый 1 день в поле Полная проверка компьютера и с помощью размещенной рядом и ставшей активной кнопки Изменить устанавливать расписание - например, каждую пятницу в 20:00. Иначе необходимо помнить о важности регулярной полной проверки и запускать ее вручную, но опять же, не реже раза в неделю В этой лабораторной работе оставьте отмеченным только флаг проверки объектов автозапуска и нажмите Далее 20. Антивирус Касперского позволяет поставить защиту паролем на ряд операций: изменения настроек, выгрузки антивируса или остановки работы компонентов и задач поиска вирусов. Если такая защита установлена, то при попытке совершить защищенную операцию будет предложено ввести пароль. Это может быть полезно, если компьютер используется несколькими пользователями и кому-то из них нельзя доверять. В этой лабораторной работе устанавливать пароли не нужно, поэтому оставьте флаг Включить защиту паролем пустым и нажмите Далее 21. На последнем этапе Мастер настройки проводит анализ Вашей системы и собирает данные об установленных программах. В дальнейшем эта информация пригодится для контроля целостности приложений, дополнительного компонента антивирусной защиты. Дождитесь окончания сбора сведений о системе 22. Следующее окно информирует, что установка завершена, но требует перезагрузки. Без перезагрузки установка Антивируса Касперского не может считаться завершенной. Поэтому убирать отметку с флага Перезагрузить компьютер можно только в исключительных случаях. В данном случае это не требуется. Оставьте отмеченным флаг Перезагрузить компьютер и нажмите Готово 23. Дождитесь завершения перезагрузки компьютера и войдите в систему под своей учетной записью 24. Обратите внимание, что после перезагрузки в правом нижнем углу экрана появилось сообщение о необходимости провести полную проверку компьютера на вирусы. О том, как настраивать такие уведомления, пойдет речь в одной из следующих лабораторных работ Заключение Эта лабораторная работа заканчивается полной установкой, включающей в себя предварительную настройку Антивируса Касперского 6.0. Если в ходе инсталляции Мастер установки не выводил сообщений об ошибках, она должна быть успешной.

**Практическая работа № 3. Настройка политики безопасности**

Цель работы: ознакомиться с методами ограничения доступа к информации

Теоретический материал Разграничение доступа является достаточно эффективным средством предупреждения возможного ущерба вследствие нарушения целостности или конфиденциальности информации. В том случае, если доступ к самому компьютеру или к его ресурсам может получить пользователь, который имеет злой умысел или недостаточный уровень подготовки, он может случайно или преднамеренно исказить информацию или уничтожить ее полностью или частично. Это же обстоятельство может привести к раскрытию закрытой информации или несанкционированному тиражированию открытой, например, программ, баз данных, разного рода документации, литературных произведений и т. д. в нарушение прав собственников информации, авторских прав… С точки зрения разграничения доступа, в информационных системах следует различать субъекты доступа и объекты доступа. В число субъектов доступа могут войти либо персонал информационной системы, либо посторонние лица. Объектами доступа являются аппаратнопрограммные элементы информационных систем. Чаще всего в качестве объектов доступа рассматриваются файлы (в том числе папки и файлы программ). Доступ к объекту может рассматриваться либо как чтение (получение информации из него), либо как изменение (запись информации в него). Тогда виды доступа определяются следующими возможными сочетаниями этих операций:

– ни чтение, ни изменение;

– только чтение;

– только изменение;

– и чтение, и изменение. Очевидно, что различие функциональных обязанностей субъектов обусловливает необходимость предоставления им соответствующих видов доступа. Управление доступом пользователей и глобальными параметрами на членах домена осуществляется на двух уровнях: локальной системы и домена. На отдельных компьютерах доступ пользователей конфигурируют на уровне локальной системы, а одновременно для нескольких систем или ресурсов, входящих в домен, — на уровне домена. Права доступа пользователя определяются руководителем организации и прописываются на рабочей станции системным администратором (администратором домена). Процедура проверки прав доступа включает авторизацию и аутентификацию. Авторизация предполагает проверку уровня доступа к объекту, а аутентификация — проверку подлинности пользователя. Для аутентификации обычно используются имя пользователя (login) и пароль (password). Системный администратор осуществляет разграничение прав доступа в соответствии с заданной системной политикой, которая предполагает: – ограничения на минимальную длину, сложность и срок действия пароля;

– требование уникальности паролей; – блокировку пользователя при неудачной аутентификации; – ограничение времени и места работы пользователя. Система разграничения доступа реализована так, что при повседневной работе пользователи не должны замечать, что любое обращение к любому объекту проходит проверку на соответствие установленным правам доступа. Списки прав доступа можно задавать на каждый документ отдельно. При создании документа автоматически задается такой доступ на него, чтобы создатель имел все права. Система разграничения доступа предназначена для реализации определенных администратором защиты правил на выполнение операций пользователями над объектами хранилища. Система ограничения прав доступа не может дать полной гарантии безопасности информации. Дело в том, что злоумышленник может получить или подобрать пароль легального пользователя. Кроме того, опытный специалист может обойти систему разграничения доступа. Средством обнаружения несанкционированного доступа к ресурсам служат системы аудита, которые автоматически фиксируют доступ к файлам и папкам и системные события. Модели разграничения доступа Наиболее распространенные модели разграничения доступа:

– дискреционная (избирательная) модель разграничения доступа;

– полномочная (мандатная) модель разграничения доступа. Дискреционная модель характеризуется следующими правилами:

– любой объект имеет владельца;

– владелец имеет право произвольно ограничивать доступ субъектов к данному объекту;

– для каждого набора субъект

– объект – метод право на доступ определен однозначно;

– наличие хотя бы одного привилегированного пользователя (например, администратора), который имеет возможность обращаться к любому объекту с помощью любого метода доступа. В дискреционной модели определение прав доступа хранится в матрице доступа: в строках перечислены субъекты, а в столбцах – объекты. В каждой ячейке матрицы хранятся права доступа данного субъекта к данному объекту. Полномочная модель характеризуется следующими правилами: – каждый объект обладает грифом секретности. Гриф секретности имеет числовое значение: чем оно больше, тем выше секретность объекта; – у каждого субъекта доступа есть уровень допуска. Допуск к объекту в этой модели субъект получает только в случае, когда у субъекта значение уровня допуска не меньше значения грифа секретности объекта. Преимущество полномочной модели состоит в отсутствии необходимости хранения больших объемов информации о разграничении доступа. Каждым субъектом выполняется хранение лишь значения своего уровня доступа, а каждым объектом – значения своего грифа секретности. Методы разграничения доступа Виды методов разграничения доступа: Разграничение доступа по спискам Суть метода состоит в задании соответствий: для каждого пользователя задается список ресурсов и права доступа к ним или для каждого ресурса определяется список пользователей и права доступа к этим ресурсам. С помощью списков возможно установление прав с точностью до каждого пользователя. Возможен вариант добавления прав или явного запрета доступа. Метод доступа по спискам используется в подсистемах безопасности операционных систем и систем управления базами данных. Использование матрицы установления полномочий

При использовании матрицы установления полномочий применяется матрица доступа (таблица полномочий). В матрице доступа в строках записываются идентификаторы субъектов, которые имеют доступ в компьютерную систему, а в столбцах – объекты (ресурсы) компьютерной системы. В каждой ячейке матрицы может содержаться имя и размер ресурса, право доступа (чтение, запись и др.), ссылка на другую информационную структуру, которая уточняет права доступа, ссылка на программу, которая управляет правами доступа и др. Данный метод является достаточно удобным, так как вся информация о полномочиях сохраняется в единой таблице. Недостаток матрицы – ее возможная громоздкость. Разграничение доступа по уровням секретности и категориям Разграничение по степени секретности разделяется на несколько уровней. Полномочия каждого пользователя могут быть заданы в соответствии с максимальным уровнем секретности, к которому он допущен. При разграничении по категориям задается и контролируется ранг категории пользователей. Таким образом, все ресурсы компьютерной системы разделены по уровням важности, причем каждому уровню соответствует категория пользователей. Парольное разграничение доступа Парольное разграничение использует методы доступа субъектов к объектам с помощью пароля. Постоянное использование паролей приводит к неудобствам для пользователей и временным задержкам. По этой причине методы парольного разграничения используются в исключительных ситуациях. На практике принято сочетать разные методы разграничений доступа. Например, первые три метода усиливаются парольной защитой. Использование разграничения прав доступа является обязательным условием защищенной информационной системы. Ход работы 1. Освоить средства разграничения доступа пользователей к папкам: – выполнить команду «Общий доступ и безопасность» контекстного меню папки (если эта команда недоступна, то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки) или команду «Свойства»; – открыть вкладку «Безопасность» и включить в отчет сведения о субъектах, которым разрешен доступ к папке и о разрешенных для них видах доступа; – с помощью кнопки «Дополнительно» открыть окно дополнительных параметров безопасности папки (вкладка «Разрешения»); – включить в отчет сведения о полном наборе прав доступа к папке для каждого из имеющихся в списке субъектов; – открыть вкладку «Владелец», включить в отчет сведения о владельце папки и о возможности его изменения обычным пользователем; – открыть папку «Аудит», включить в отчет сведения о назначении параметров аудита, устанавливаемых на этой вкладке, и о возможности их установки обычным пользователем; – закрыть окно дополнительных параметров безопасности. 2. Освоить средства разграничения доступа пользователей к файлам: – выполнить команду «Свойства» контекстного меню файла; – повторить все задания п. 1, но применительно не к папке, а к файлу. 3. Освоить средства разграничения доступа к принтерам: – выполнить команду «Принтеры и факсы» меню «Пуск»; – выполнить команду «Свойства» контекстного меню установленного в системе принтера; – повторить все задания п. 1, но применительно не к папке, а к принтеру. 4. Освоить средства разграничения доступа к разделам реестра операционной системы:

- с помощью команды «Выполнить» меню «Пуск» запустить программу редактирования системного реестра regedit (regedt32);

– с помощью команды «Разрешения» меню «Правка» редактора реестра определить сведения о правах доступа пользователей к корневым разделам реестра, их владельцах и параметрах политики аудита;

– включить в отчет сведения о правах доступа пользователей к данной папке и о ее владельце.

**Практическая работа № 4 Настройка программы-браузера**

Цель работы: изучить способы настройки браузера Теоретический материал Браузер – это программа для просмотра web-страниц. Настройка браузера. Все браузеры позволяют выполнить некоторые настройки для оптимизации работы пользователей в Интернете. В браузереInternet Explorer основная часть настроек содержится в меню Сервис – Свойства обозревателя. Вкладка Общие позволяет задать адрес домашней страницы, которая будет автоматически загружаться в окно браузера при его запуске, цвета гиперссылок по умолчанию, название шрифта по умолчанию. Здесь же определяется сколько дней будет храниться ссылка посещенных страниц в журнале. Кроме того, для ускорения просмотра. Все посещенные страницы помещаются в специальную папку, и с помощью кнопки Параметры можно задать разные способы обновления таких страниц. С помощью вкладки Безопасность можно создать списки надежных узлов и узлов с ограниченными функциями. Зона Интернет будет при этом включать все остальные узлы, не вошедшие в эти две папки. Для каждой из них с помощью кнопки Другой можно изменить параметры безопасности, установленные для них по умолчанию. Здесь можно запретить выполнение сценариев, отображение всплывающих окон, загрузку файлов и т.д. Вкладка Конфиденциальность дает возможность настроить работу с файлами cookie, с помощью которых информация о пользователе автоматически передается на сервер. Вкладка Содержание позволяет ограничить доступ к некоторой информации (насилие, ненормативная лексика и т.д.). Вкладка Подключения позволяет установить подключение к Интернету. На вкладке Дополнительно можно задать некоторые дополнительные параметры работы (отключить загрузку графических изображений, отменить подчеркивание ссылок, запретить отладку сценариев и т.д.). Вкладка Программы позволяет определить программы, которые будут по умолчанию использоваться службами Интернета (почтовые программы,html-редакторы и т.п.). Ход работы 1. Создайте папку на рабочем столе и переименуйте её. 2. Откройте броузер Internet Explorer. 3. На вкладке Панели инструментов меню Вид уберите все флажки напротив всех панелей инструментов. 4. В меню Вид уберите флажок со вкладки Строка состояния. 5. Нажмите кнопку Print Screen. 6. Откройте графический редактор и вставьте скопированное в рабочую область. Настройка панелей инструментов Internet Explorer. 7. Вернитесь к обозревателю и при помощи действий Вид◊ Панели инструментов, отобразите на экране Ссылки. Скопируйте в Paint данное окно, сравните с предыдущим рисунком и вырежьте все части, которые дублируют первый рисунок. Вставьте получившееся на фон рабочей области рисунка и подпишите «ссылки».

Вернитесь снова к обозревателю и, проделав аналогичные действия, вставьте в тот же рисунок Адресную строку, Обычные кнопки, строку состояния и подпишите их. Скопируйте аналогичным образом Панели обозревателя: Избранное (часто посещаемые веб-страницы), Журнал (список недавно посещённых веб-страниц), Поиск, Папки. 8. Для просмотра веб-страницами вам нужно научиться изменять размер шрифта, отключить графику для увеличения скорости отображения всех веб-страниц. Для того, чтобы установить оптимальный для просмотра страницы размер шрифта, нужно сделать следующее Вид◊Размер шрифта. Выберите Самый крупный. 9. Чтобы отключить графику для увеличения скорости отображения всех веб-страниц, меню Сервис обозревателя Internet Explorer выберите команду Свойства обозревателя. 10. Выберите вкладку Дополнительно. В группе Мультимедиа снимите один или несколько из флажков: Отображать рисунки, Воспроизводить анимацию на веб-страницах, Воспроизводить видео на веб-страницах и Воспроизводить звуки на вебстраницах. 11. Чтобы увеличить размер дискового пространства, выделяемого для временного хранения веб-страниц, в менюСервис обозревателя Internet Explorer выберите команду Свойства обозревателя. 12. На вкладке Общие нажмите кнопку Параметры. 13. Чтобы увеличить размер дискового пространства, выделяемого для временного хранения страниц, переместите движок вправо.

**Практическая работа № 5 Работа с реестром**

Цель работы: изучить структуру ключей реестра, типы параметров ключей, способы редактирования реестра; получить практические навыки работы с редактором реестра RegEdit. Теоретический материал Структура и основные принципы работы с реестром Реестр (Registry) – это системная база данных Windows . Она является хранилищем множества параметров и установок, необходимых для нормального функционирования Windows на данном конкретном компьютере. Реестр – это не статическая база данных настроек, он работает постоянно и постоянно обновляется. Не существует двух одинаковых реестров. Файлы системного реестра База данных системного реестра Windows 95 хранится в двух файлах – System.dat и User.dat. Это скрытые системные файлы, доступные только для чтения. Данные хранятся в них в двоичном виде и не могут быть просмотрены при помощи обычного текстового редактора. Для внесения изменения в реестр должен использоваться специальный редактор Regedit.exe, который изображает эти два файла как одну систему. По умолчанию файлы System.dat и User.dat хранятся в папке \Windows. В файле System.dat хранятся сведения об аппаратуре, на котором работает система Windows, а также об установленном на нем программном обеспечении. Значения, хранящиеся в этом файле, автоматически изменяются при изменении аппаратной конфигурации, а также при установке и удалении приложений. В файле User.dat хранится информация, относящаяся к пользователю. В частности, это могут быть данные о «чувствительности» мыши, цветовой схеме, курсорах, шрифтах, клавиатуре и прочем. В этом же файле находятся сведения о конфигурации рабочего стола и сети для разных пользователей – так называемые пользовательские конфигурации. Аналогичные файлы для хранения базы данных системного реестра существуют и в других ОС семейства Windows 9х/NT. Отличаться могут количество и, соответственно, названия файлов.

Редактор реестра Фирма Microsoft предусмотрела множество элементов интерфейса пользователя, предназначенных для изменения конфигурации системы , т.е. реестра – это и Панель Управления (Control Panel), и диалоговые окна свойств, и многое другое. При этом изменения параметров отражаются на функционировании системы немедленно. Вместе с тем в некоторых случаях этого оказывается недостаточно. Однако, изменять системный реестр, используя редактор реестра, следует только в том случае, когда это действительно необходимо. Если вы редактируете базу данных реестра, то для того, чтобы хранящиеся в ней параметры были прочтены в память и вступили в силу, чаще всего необходимо перезапустить компьютер. Для запуска редактора реестра следует выполнить команду Пуск - Выполнить- RegEdit. Файл запуска реестра RegEdit.exe всегда находится в папке \ WINDOWS. Объекты системного реестра Реестр содержит три типа объектов: ключи, параметры и значения. Ключи - вершина иерархической структуры реестра. Под ключами реестра могут располагаться другие узлы иерархического дерева (подключи). Кроме этого, каждый ключ может содержать один или несколько параметров. Все ключи и параметры в пределах подключа должны иметь уникальные имена. Параметры имеются у каждого ключа и подключа. У каждого ключа обязательно есть хотя бы один параметр -" По умолчанию". Если значения параметров не заданы, то они имеют значение Null. Параметры состоят из трех частей: тип параметра, имя параметра и его значение. Допустимы следующие типы параметров: двоичные, двойное слово и строковые. Каждому типу параметров соответствует своя пиктограмма в окне редактора реестра. String (строковое). Представляет из себя ASCIIZ–строку (заканчивается символом с кодом 0). Имеет переменную длину, максимальный размер 64 кБ. Значение строки всегда заключается в кавычки. Binary (двоичное). Максимальный размер 64 кБ. В окне редактора реестра представлено в виде 16-ричного значения. DWORD (двойное слово). Представляет собой число размером 32 бита (в реестре 8-значное шестнадцатеричное число). Чтобы отличить этот тип данных от двоичного, перед численным значением DWORD всегда есть два символа: 0х. Структура системного реестра Вся база системного реестра разделена на шесть основных разделов, которые принято называть ветвями. Каждая ветвь содержит в себе параметры, относящиеся к определенному набору ключей. Ниже кратко описано назначение этих разделов. [HKEY\_CLASSES\_ROOT] Содержит сведения о встраивании и связывании объектов (Object Linking and Embedding, OLE) и ассоциации файлов с приложениями. [HKEY\_USERS] Содержит информацию обо всех пользователях данной рабочей станции. Здесь хранятся данные о каждом пользователе, а также типовые настройки, служащие шаблоном для новых ключей, создаваемых пользователем. Типовые настройки включают различные значения по умолчанию для программ, событий, конфигураций рабочего стола и т.д. [HKEY\_CURRENT\_USER] Содержит настройки системы и программ, относящиеся к текущему пользователю. Он создается при регистрации пользователя в системе на основе информации из соответствующего ключа [HKEY\_USERS]. Именно здесь хранится информация о том, как данный пользователь сконфигурировал рабочую станцию. [HKEY\_LOCAL\_MACHINE] Содержит спецификации рабочей станции, драйверов и др. системные настроцки, включая информацию о типах установленного оборудования, настройках портов конфигурации программного обеспечения. Эта информация специфична для компьютера, а не для пользователя.

[HKEY\_CURRENT\_CONFIG] Содержит информацию о текущей конфигурации аппаратуры компьютера, используется в основном на компьютерах с несколькими аппаратными конфигурациями, например, при подключении портативного ПК к стыковочной станции и отключении от нее. Информация , содержащаяся в этом ключе, копируется из ключа [HKEY\_LOCAL\_MACHINE]. [HKEY\_DYN\_DATA] Содержит динамическую информацию о состоянии различных устройств, причем она создается заново при каждом старте системы. Этот ключ используется как часть системы измерения производительности и для конфигурации устройств Plug-and-Play. Состав основных разделов Каждый из вышеперечисленных разделов содержит в себе другие разделы — как и файловая система, Registry имеет структуру дерева. Каждый узел (раздел или подраздел) называется ключом.

Hkey\_Classes\_Root Структура раздела несколько отличается от всех остальных. Для каждого зарегистрированного расширения файла имеется подключ (например, .bmp). Значение этого ключа "По умолчанию" указывает на подключ описания документа ("ACDC\_BMP"), который расположен в той же ветви основного раздела. В подключе описания документа и содержится цепочка ключей, хранящих информацию об ассоциациях, OLE, DDE. Hkey\_Local\_Machine Информация, сохраненная здесь, используется приложениями, устройствами и системой, и не зависит от того, кто был заявлен в качестве пользователя. Устройства могут помещать информацию в системный реестр с помощью Р1ug&Рlау-интерфейса, программные средства — посредством стандартного API. Подраздел Config

• Содержит информацию о различных конфигурациях аппаратных средств.

• Каждая конфигурация имеет уникальное обозначение и хранится в отдельном подразделе с соответствующим именем.

• Конфигурации перечислены в списке в окне утилиты Система. Здесь же их можно обрабатывать.

• При запуске Windows проводится проверка конфигурации аппаратных средств. При этом может произойти следующее:

• В большинстве случаев конфигурационные данные позволяют Windows автоматически выбрать соответствующую конфигурацию.

• При первом после изменения оборудования запуске компьютера Windows создает новый элемент конфигурации для новых конфигурационных данных. В результате создается и новый Config-элемент в системном реестре. • Когда конфигурационные данные не позволяют системе Windows однозначно решить, какую из описанных конфигураций следует выбрать, пользователю при загрузке системы предлагается меню, посредством которого он может выбрать подходящую конфигурацию. Подраздел Enum

• Windows располагает специальными программами, которые отвечают за построение дерева аппаратуры в системном реестре (например, Диспетчер устройств, вызываемый через Панель управления - Система- Устройства).

• Каждому устройству присваивается уникальный идентификационный код.

• В системном реестре хранится идентификационная информация о каждом устройстве, например, тип устройства, идентификационный код (ID) устройства, информация об изготовителе и информация о драйвере. Информация о составе данного раздела приведена в табл.2. Подраздел Software

• Содержит информацию о каждом программном средстве, установленном на компьютере.

• Содержимое этого раздела является общим для всех пользователей данного компьютера.

• Hkey\_Local\_Machine\Software содержит ряд подразделов и сведения о различных подразделах (их описание), которые могут появиться в системном реестре (см.табл.3). Подраздел System

• Данные в подразделе System содержат все параметры драйверов устройств и служб, используемые при запуске Windows.

• Вся информация хранится в подразделе CurrentControlSet. Он содержит два следующих подраздела:

• Control: Подраздел включает информацию, используемую, при запуске системы, например, сетевое имя компьютера и запускаемые подсистемы. • Services: Подраздел включает информацию, необходимую для контроля загрузки и конфигурирования драйверов, файловой системы, и др. Здесь также определяется, как отдельные службы вызывают одна другую. Состав двух вышеназванных подразделов приведен в табл.4 и 5. Hkey\_Current\_User и Hkey\_Users

• Содержит Default-подраздел и подразделы для всех пользователей, заявленных в системе.

• Информация из подраздела Default используется для того, чтобы создать конфигурацию для нового пользователя.

• Hkey\_Current\_User содержит информацию о пользователе, работающем на компьютере в текущем сеансе (см. табл.6). Если существуют одинаковые параметры в Hkey\_Local\_Machine и Hkey\_Current\_User, то используются значения параметров, взятые из Hkey\_Current\_User. Hkey\_Current\_Config и Hkey\_Dyn\_Data

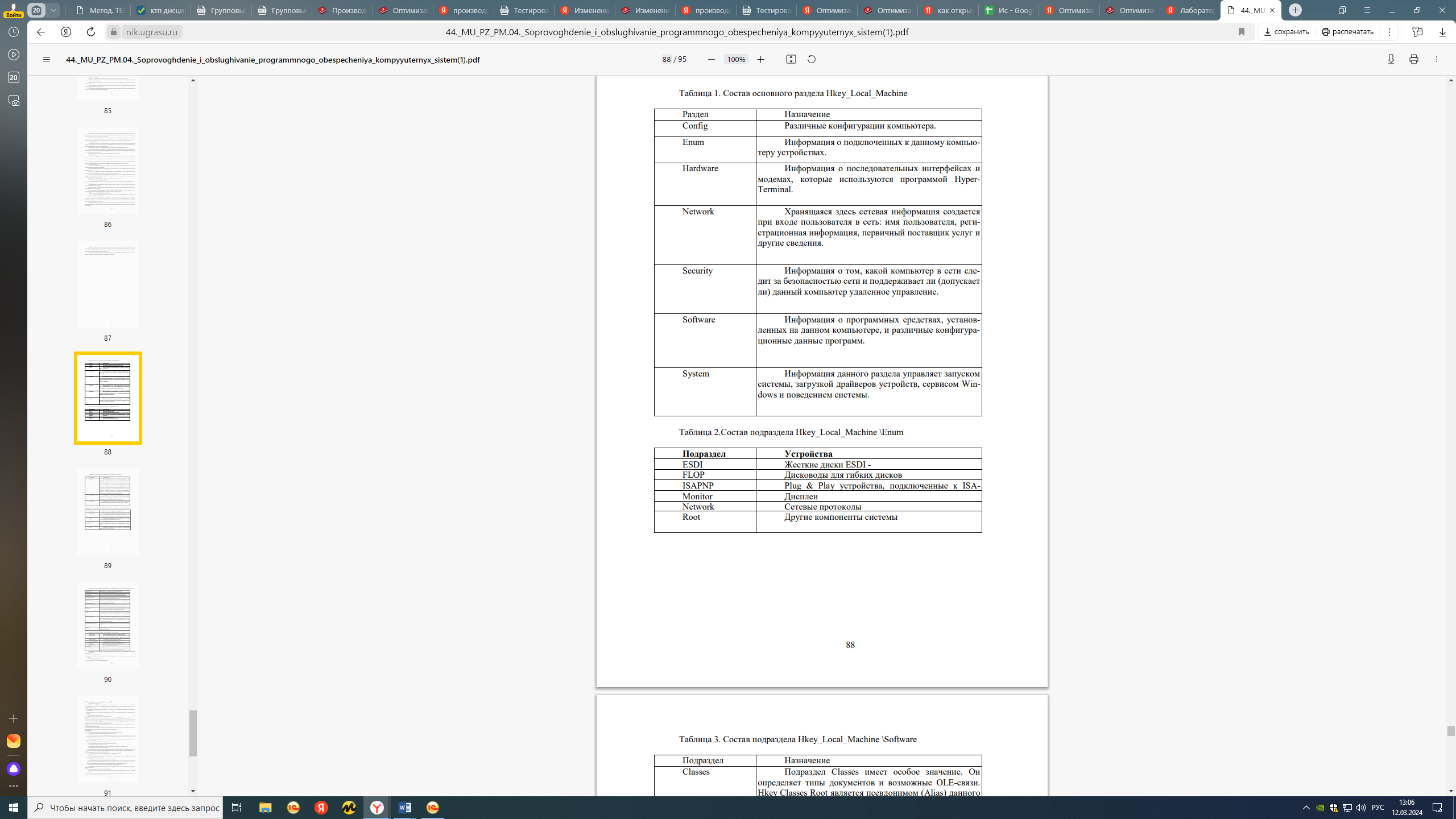
• Hkey\_Current\_Config указывает на текущую системную конфигурацию, которая сохранена в Hkey\_Local\_Machine\Config.

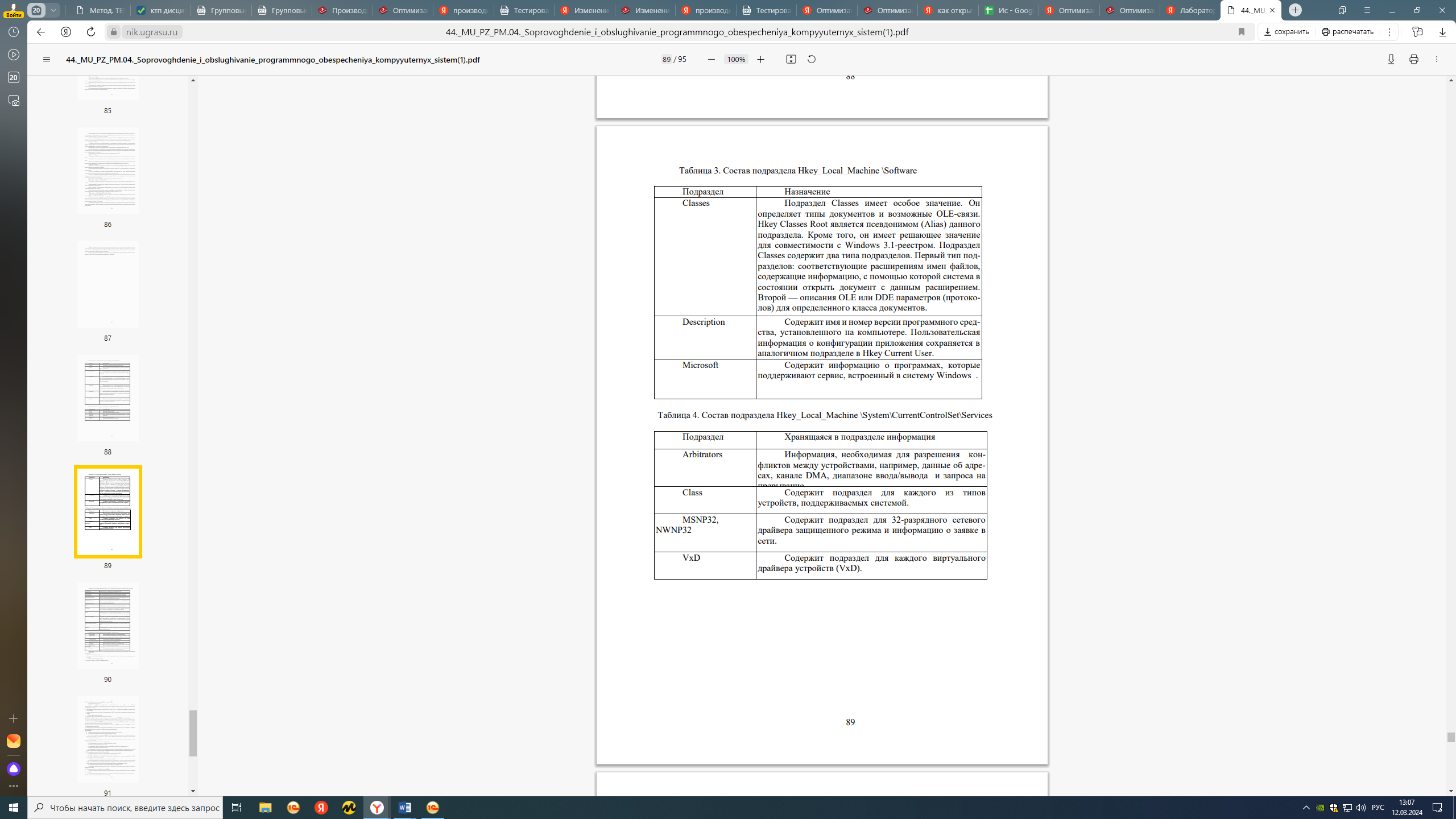
• Часть системной информации в Windows должна постоянно присутствовать в оперативной памяти, поскольку системе необходим быстрый доступ к этой информации и Windows не может ожидать, пока нужные данные будут прочитаны с жесткого диска. Вся эта информация находится в Hkey\_Dyn\_Data.

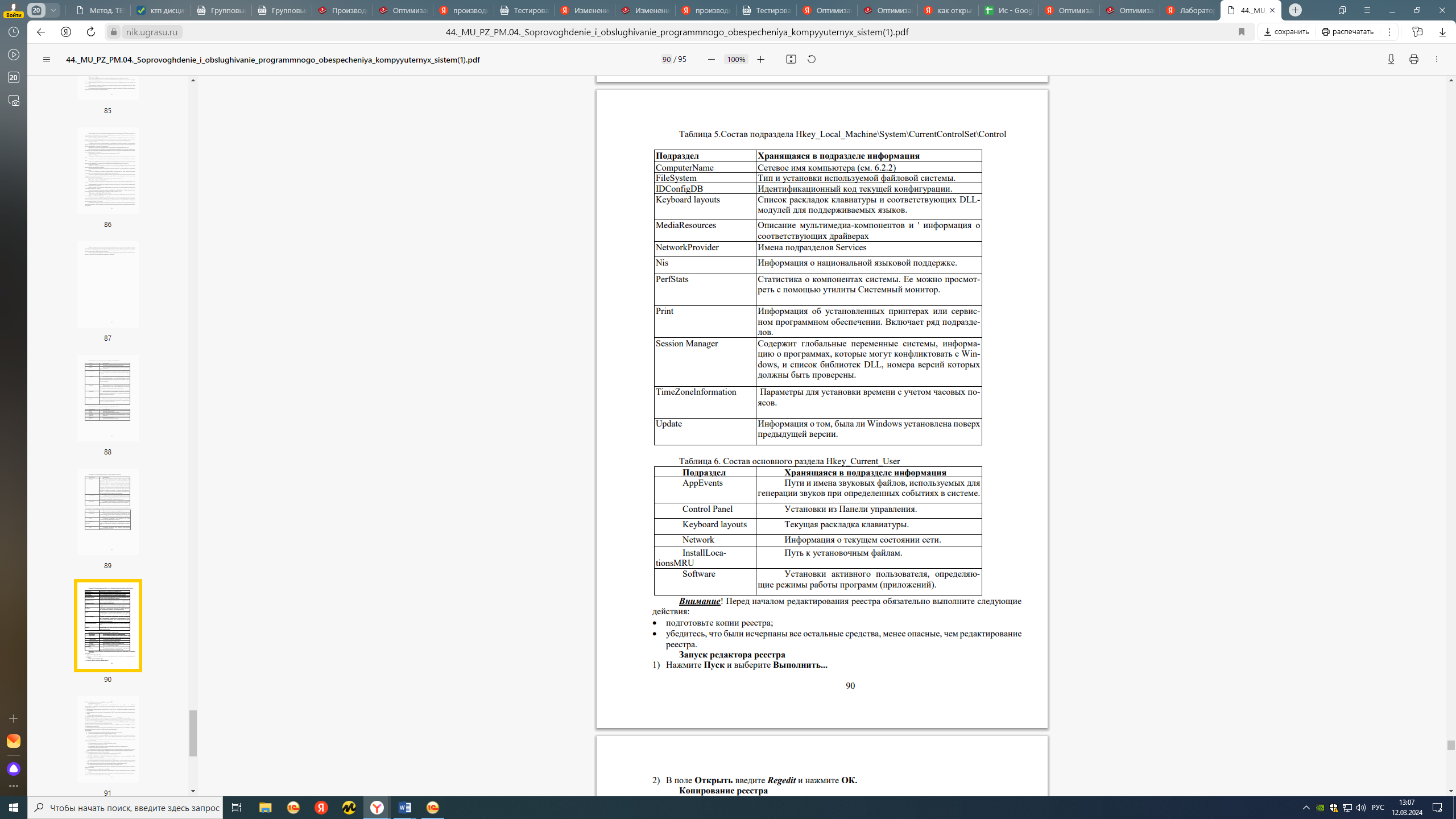
• Подраздел Hkey\_Dyn\_Data\Configuration Manager, называемый также деревом аппаратуры, представляет собой хранящееся в оперативной памяти описание текущей системной конфигурации.

• Дерево аппаратуры создается заново при каждом запуске системы и адаптируется, если в состав или конфигурацию аппаратуры были внесены изменения. Присутствующие в этом разделе данные можно просмотреть с помощью Редактора реестра, они всегда соответствуют текущему состоянию аппаратуры компьютера.

• Hkey\_Dyn\_Data содержит статистическую информацию о различных сетевых компонентах в системе. Она находится в подразделе PerfStats.







2) В поле Открыть введите Regedit и нажмите ОК. Копирование реестра Копии реестра создаются автоматически в ОС в файлах System.DA0 и User.Da0. Для принудительной создании копии реестра можно использовать следующие методы:

• скопировать файлы реестра (System.DAТ и User.DАТ в . Windows95) в файлы с любым другим именем;

• экспортировать реестр в файл с расширением .REG, используя возможности редактора реестра. Восстановление реестра 1) Нажмите Пуск и выберите Завершение работы... 2) Выберите Перезагрузить компьютер в режиме эмуляции MS-DOS и нажмите Да. 3) После перезагрузки выполните копирование файлов System.DA0 и User.Da0 в файлы System.Dat и User.Dat . Перед копированием для изменения атрибутов файлов реестра используйте внешнюю команду DOS- ATTRIB, которая находится в каталоге C:\ Windows. После копирования восстановите снятые атрибуты файлов реестра. 4) Для получения справки по использованию команды ATTRIB запустите ATTRIB с ключом ? в командной строке DOS. 5) Перезагрузите компьютер. Теперь системный реестр находится в том состоянии, в котором он находился при последнем успешном запуске компьютера. Ход работы 1) Выполнить резервное копирование файлов системного реестра. 2) Изучить функции редактора реестра Registry Editor: a) создать новый ключ в разделе Hkey\_Current\_config, создать для него параметр строкового типа и задать его значение –"Мой"; какой параметр для вновь созданного ключа появляется по умолчанию? В отчете указать иерархию ключа, названия и значения созданного параметра и параметра по умолчанию. b) удалить созданные ключ и параметр; c) найти первых два ключа с полным именем "Setup" ; в отчете указать иерархию ключа. d) проверить, имеет ли реестр ключ со значением любого его параметра 35; отразить результата поиска в отчете; e) проверить возможность экспортировать реестр в новый файл и импортировать его из ранее сохраненного файла; какое расширение имеют файлы импорта-экспорта реестра? 3) Исследование раздела Hkey\_Clauses\_Root. a) Найти ссылку на подключ для файлов с расширением DOC. b) Найти подключ, на который указывает эта ссылка. c) Для найденного подключа определить следующие ключи настройки Word: вид графического значка (icon); командная строка для запуска исполняемого файла. d) Отредактировать значения параметра "По умолчанию" для этих двух ключей таким образом, чтобы изменился графический значок Word , а также изменилось приложение, которое автоматически запускается при открытии файлов с расширением Doc. e) Проверить выполненные установки, открыв любой файл Doc. В отчете указать иерархию двух ключей, название исследуемых параметров, их новое и старое значения. 4) Исследование раздела Hkey\_Local\_Machine. Найти подключи конфигурации оборудования. Сколько конфигураций имеет данный компьютер? В отчете указать иерархию ключа, название исследуемого параметра, его значения. 5) Исследование раздела Hkey\_Current\_config

a) Копией какого ключа является данный раздел? b) Найти ключ, отвечающий за настройки дисплея. c) Ознакомиться со списком параметров этого ключа. d) Изменить текущую разрешающую способность монитора на значение "640,480". e) Для проверки выполнения перегрузить операционную систему (ОС). В отчете указать иерархию ключа, название исследуемого параметра, его новое и старое значения. 6) Исследование раздела Hkey\_Current\_user. a) Копией какого ключа является данный раздел? b) Найти ключ, отвечающий за настройки Рабочего стола. Ознакомиться со списком вложенных ключей . Для произвольно выбранных из списка 5 ключей исследовать, аналогом каких настроек Панели управления они являются. В отчете указать иерархию пяти ключей и соответствующие настройки Панели управления. c) Изменить с помощью реестра ширину полосы прокрутки и строки командного меню в окнах Windows. Проверить выполненные настройки. В отчете указать иерархию ключа, название исследуемого параметра, его новое и старое значения. d) В подразделе установленного программного обеспечения для текущего пользователя найти ключ, хранящий полное имя файла справки Word. В отчете указать иерархию ключа. e) Для приложения Word найти ключ, хранящий информацию о каталоге автоматически сохраняемых документов. Сравнить его с каталогом, указанным в параметрах Word. (Запустить Word, вызвать Сервис-Параметры - Расположение-Автосохраненные). Иерархию ключа и результаты сравнения отразить в отчете. Проверить влияние изменения параметров приложения Word через меню Сервис на значение параметра автосохранения ключа в реестре, а также обратную связь. В отчете указать иерархию ключа, название исследуемого параметра. f) Для приложения Excel найти ключ, хранящий информацию о последних 9 загруженных файлах XLS. Запомнить названия параметров и значение одного из них. Информацию о ключе, параметре и его значении отразить в отчете. 7) Восстановить состояние системного реестра из резервных копий или из копий ОС

**Практическая работа № 6.** **Работа с программой восстановления файлов и очистки дисков**

Цель работы: изучение работы программ восстановления файлов и очистки дисков Ход работы Задание 1. Используя задания Сведения о системе, определите следующие параметры компьютерной системы: Мультимедиа, запоминающие устройства, системные драйверы, группы программ, автоматически загружаемые программы. Для запуска программы Сведения о системе выберите в меню Пуск команду Программы-Стандартные-Служебные-Сведения о системе. Для получения сведений об устройствах мультимедиа выберите в дереве категорий в левой области окна программы категорию Компоненты, а в ней подкатегорию Мультимедиа. Выбирая в этой подкатегории элементы мультимедиа аудио- и видеокодеки, CD-ROM, звуковое устройство, дисплей, просмотрите в правой части окна программы сведения, относящиеся к элементу, выделенному в дереве категорий.

Для просмотра сведений о запоминающих устройствах выберите в левой части окна категорию Запоминающие устройства. Выбирая в этой категории различные подкатегории, в области сведений просмотрите информацию об устройствах внешней памяти. Для просмотра сведений о системных драйверах выберите категорию Программная среда, а в ней подкатегорию Системные драйверы. Для просмотра данных о группах программ найдите в категории Программная среда подкатегорию Группы программ, чтобы вывести сведения о них в правой области окна. Аналогично найдите сведения о программах, автоматически загружаемых при старте Windows XP. Закройте окно программы Сведения о системе. Задание 2. Используя стандартную программу Windows Проверка диска, проверьте диск А: на наличие поврежденных секторов и ошибок файловой системы. При этом если будут обнаружены ошибки, то задайте режим восстановления поврежденных секторов диска автоматического исправления системных ошибок. Перед запуском проверки диска закройте все файлы на нем. Открыв окно Мой компьютер, выберите локальный диск А:, затем в меню Файл выберите команду Свойства. На вкладке Сервисв группе Проверка диска нажмите кнопку «Выполнить проверку». В группе Параметры проверки диска установите флажки Автоматически исправлять системные ошибки и Проверять и восстанавливать поврежденные сектора. Для начала процесса сканирования диска на наличие ошибок щелкните на кнопке «Запуск». По окончании проверки диска на экран будет выведено сообщение об окончании проверки диска. 3. Используя стандартную программу Очистка диска, выполните очистку диска С:. Для запуска программы выберите в меню Пуск команду Программы-СтандартныеСлужебные-Очистка диска. В рабочем окне программы выберите логический диск С:, который будет подвергнут процедуре очистки, и щелкните на кнопке «ОК». После этого мастер очистки диска перейдет к процедуре проверки состояния файлов на данном диске. После завершения анализа текущего состояния диска программа представит Отчет о проделанной работе, указав, сколько места можно освободить. Определив, что подлежит удалению при очистке диска, щелкните на кнопке «ОК», а затем подтвердите удаление файлов при очистке диска, щелкнув на кнопке «Да». После этого запускается процесс очистки диска. 4. Используя стандартную программу Дефрагментация диска, выполните оценку фрагментированности файлов на диске С: и, если требуется, то выполните дефрагментацию этого диска. Для запуска программы Дефрагментации диска выберите в меню Пуск команду Программы-Стандартные-Служебные-Дефрагментация диска. После этого выберите диск С: и нажмите кнопку «Анализ». По завершении анализа тома программа дефрагментации диска выведет результаты анализа и сообщение о том, нуждается ли данный том в дефрагментации. Если в окне сообщения программа рекомендует выполнить дефрагментацию диска, то щелкните на кнопке «Дефрагментация», если иначе - щелкните кнопку «Закрыть». Если была запущена процедура дефрагментации, то после ее окончания результаты будут отображены в графическом представлении с цветовой кодировкой в полях результатов анализа и дефрагментации. Чтобы просмотреть подробный отчет о дефрагментации, нажмите кнопку «Вывести отчет». Закройте окно программы Дефрагментация диска. Задание 3. Используя служебную программу Архивация данных, архивируйте данные из папки C:\Program Files\Microsoft Office\Templates в архив с именем Templates на диске D:. Для запуска приложения Архивация данных выберите в меню Пуск команды Программы-Стандартные-Служебные-Архивация данных. Если программа архивации запускается в режиме мастера, то для переключения в расширенный режим нажмите кнопку «Расширенный» в окне мастера архивации.

Для архивации выбранных файлов и папок на жестком диске перейдите на вкладку Архивация и установите флажок в списке Установите флажки для папки C:\Program Files\Microsoft Offlce\ Templates, данные из которой вы хотите заархивировать. Задайте в качестве носителя диск D: и имя файла для архива Templates, нажмите на кнопку «Архивировать», а затем в окне Сведения о задании архивации выберите вариант Затереть данные носителя этим архивом. Щелчком на кнопке «Архивировать» запустите процедуру архивации. После этого в окне Ход архивации пронаблюдайте за процессом архивации, по окончании которого будет выведено окно сообщения о завершении архивации с краткими сведениями. Для просмотра подробного текста отчета щелкните на кнопке «Отчет». Задание 4. Используя служебную программу Архивация данных, создайте архив системных файлов и дискету аварийного восстановления, которые могут быть использованы в целях восстановления системы в случае ее отказа. Приготовьте чистую дискету емкостью 1,44 Мбайта для сохранения параметров системы, затем запустите приложение Архивация в режиме Расширенный. В меню Сервис выберите команду Мастер аварийного восстановления системы. Следуйте инструкциям, появляющимся на экране. Для перехода к следующему шагу мастера щелкайте на кнопке «Далее». Выбрав тип носителя для системного архива и имя носителя для хранения архивных данных, например, D:\Arxiv\Backup.bkf, щелкните на кнопке «Далее» для создания архива. После этого будет выполнена архивация системных файлов, необходимых для загрузки системы, и создание дискеты аварийного восстановления. По окончании процесса архивации в ответ на предложение вставить дискету вставьте чистую дискету, после этого будет создана дискета аварийного восстановления. Для просмотра подробного отчета щелкните на кнопке «Отчет». Закройте окно программы Архивация данных.