Стариченко Е.Б.

НЕКОТОРЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СРЕДЫ ВУЗА

old@uspu.ru
ГОУ ВПО Уральский государственный педагогический университет
г. Екатеринбург

В настоящее время трудно переоценить значение сетевых и коммуникационных технологий и их роль в развитии общества. Умение пользоваться ими как для поиска необходимой информации, так и для организации взаимодействия с окружающими, становится элементом информационной культуры современного человека. Однако её формирование по-прежнему остаётся достаточно сложной задачей. Эта проблема касается как людей, получивших образование достаточно давно, так и современных студентов, выросших рядом с компьютером.

Следствием пренебрежения элементарными правилами информационной безопасности чаще всего являются локальные эпидемии компьютерных вирусов, что приводит к снижению работоспособности сети учебного заведения, к отказам и простоям в работе оборудования, к потере важных данных. Опыт администрирования кампусной сети Уральского государственного педагогического университета показывает, что пользователи всецело полагаются на установленную антивирусную программу, считая, что одного факта наличия её на компьютере вполне достаточно для полноценной защиты. При этом совершенно не принимается во внимание необходимость выполнения стандартных и простых действий по проверке носителей и жёсткого диска, а также элементарные правила работы с электронной почтой. В значительной степени это касается работников, достаточно давно закончивших образование, для которых компьютер до сих пор не стал полноценным рабочим инструментом.

Для разрешения сложившейся ситуации, управлением информатизации УрГПУ принимаются меры в различных направлениях. С одной стороны в течение учебного года постоянно действуют и регулярно проводятся курсы повышения квалификации профессорско-преподавательского состава и административных работников, на которых сотрудникам объясняют основы информационной культуры, обучают их работе с базовыми программными средствами, акцентируя внимание на правильном и систематическом использовании антивирусных пакетов.

Защита сети техническими средствами является другим направлением деятельности сотрудников нашего управления. В 2008 году в значительной степени реорганизована кабельная система, созданы активные узловые точки, в которых расположены управляемые коммутаторы. Все узлы соединены магистральными линиями с центральным коммутатором. Такая схема, невозможная на начальном этапе создания сети (как по финансовым, так и по временным причинам), позволила предоставить каждому пользователю персональный порт, логически разделить всё сетевое пространство на виртуальные подсети, контролировать и легко определять источник паразитного трафика, порождаемого вредоносными программами. Разделение пользователей по виртуальным сетям осуществляется по подразделениям или кабинетам. Это позволяет сохранить привычную и комфортную обстановку для работы, когда коллеги, работая над решением одной производственной задачи, обмениваются документами, предоставляя к ним общий доступ. С точки зрения безопасности такой подход позволяет ограничить ареал распространения вирусов одной виртуальной сетью, а также блокировать распространение широковещательного трафика за её пределы.

Со времени начала работ по реорганизации сети УрГПУ значительно устойчивее стала работать сеть, прекратились отказы на обслуживание абонентов со стороны оборудования, стабилизировалась скорость доступа к внешним и внутренним ресурсам.

Таким образом, решение проблемы недостаточной информационной культуры работников вуза должно вестись по нескольким направления, что повышает результативность принимаемых мер как технического, так и организационного характера.

Шамонин Е.Д.

ЗАЩИТА ПРИВАТНОЙ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

shamonined@mail.ru
Уральский государственный университет (УрГУ)
г. Екатеринбург

Практически любой вид деятельности, в том числе научная и преподавательская, в настоящее время немыслима без использования в том или ином виде средств вычислительной техники (СВТ) и информационных технологий (ИТ). Использование для такой деятельности многопользовательских автономных рабочих мест (АРМ), либо рабочих мест в составе сети, неизмеримо повышает ее эффективность, но неизменно влечет за собой вопросы, связанные с необходимостью обезопасить приватную информацию от доступа со стороны посторонних лиц. Однако далеко не каждый преподаватель на рабочем месте имеет в своем полном распоряжении персональный компьютер, на котором вопрос защиты конфиденциальной информации решается достаточно просто. И речь здесь не идет о системах защиты от несанкционированного доступа (НСД), реализованных путем активации защитных функций BIOS (Basic Input/Output System, базовая система ввода/вывода) или установкой сложного пароля на вход в операционную систему.

В первом случае (рисунок 1) – установка пароля на загрузку операционной системы (ОС) и пароля на возможность изменения настроек BIOS SETUP – просто осуществляется разбиение всех пользователей на две группы: тех, кто знает парольную информацию, и тех, кто ее не знает. А это не является полноценным комплексом идентификации/аутентифика-ции, когда пользователь представляется системе под тем именем, под которым он ей известен и подтверждает, что он именно тот, за кого себя выдает.

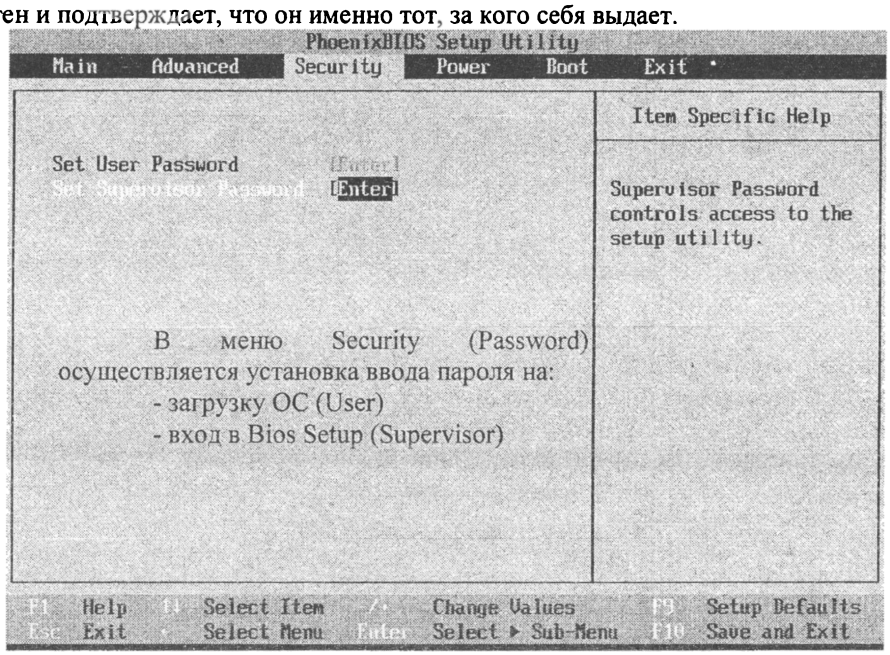

Рисунок 1 – Установка паролей User Password и Supervisor Password в настройках BIOS

Да и методов обхода такой защиты выработано немало – начиная с банального обнуления микросхемы CMOS (перепрограммируемая часть BIOS) тем или иным способом, и заканчивая таким экзотическим, как замена этой микросхемы на другую, аналогичную, заранее подготовленную злоумышленником.

Парольная защита, реализованная в самой операционной системе, также не может дать высокой гарантии того, что злоумышленник не получить доступ к конфиденциальным данным. Начиная с того, что с использованием мощных современных вычислительных средств достаточно просто реализуется подбор пароля путем простого перебора («атака в лоб»). Существует возможность перехвата пароля путем простого наблюдения, либо с использованием программных/аппаратных перехватчиков паролей. Заканчивая загрузкой «гостевой» операционной системы со сменного носителя с последующим доступом к содержимому стационарного жесткого диска. В связи с этим настоящее время началось внедрение систем, которые осуществляют процедуры идентификации/аутентификации по биологическим признакам. Производители предлагают готовые решения для операционных систем Windows XP/Vista, позволяющие проводить эти процедуры, например, по отпечатку пальца (рисунок 2) или по трехмерной карте лица (рисунок 3).

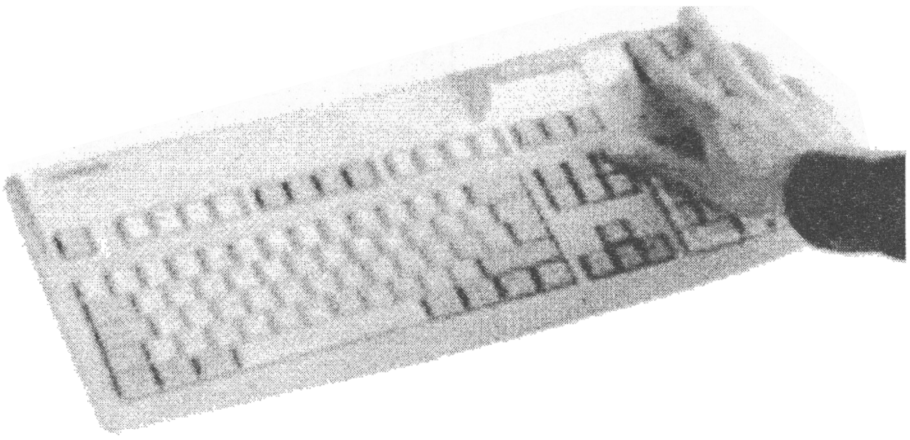

Рисунок 2 – Варианты исполнения дактилоскопических сканеров: а, в – выносные дактилоскопические сканеры; б, г – сканеры, встроенные в манипулятор «мышь» и клавиатуру

Однако такие варианты защиты от НСД являются достаточно дорогостоящими с одной стороны, а с другой стороны легко обходятся элементарным извлечением жесткого диска из системного блока с последующим его к другому компьютеру.

Поэтому полную гарантию защиты информации от НДС дает только изъятие на время отсутствия легального пользователя основного носителя информации (жесткого диска) из системного блока и помещение его в тайник, сейф, либо другое, недоступное для посторонних, место. Такое решение не требует больших финансовых и временных затрат, поскольку на рынке широко представлены различные варианты недорогих устройств, позволяющих быстро монтировать/демонтировать жесткий диск в системный блок компьютера (рисунок3). Причем, такой вариант позволяет как хранить отдельно от системного блока как жесткий диск с установленной операционной системой и приватными данными (рисунок 4,а), так и просто жесткий диск с конфиденциальной информацией (рисунок 4,б).

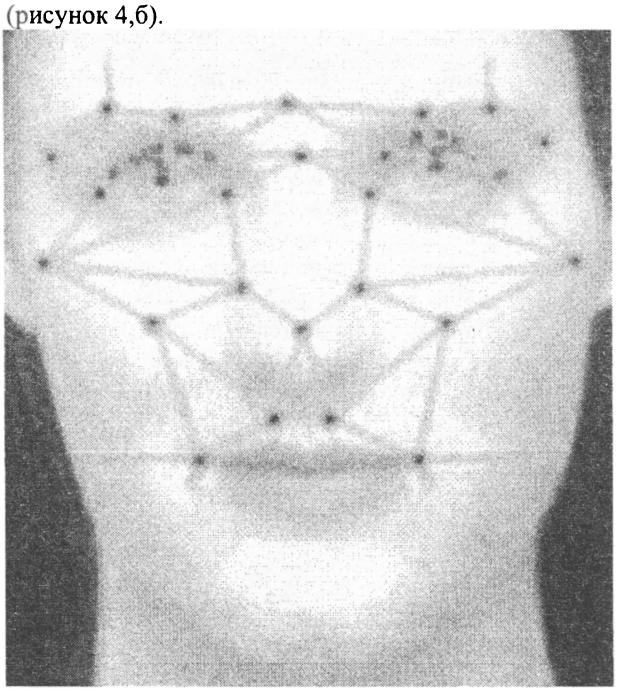

Рисунок 3 – Построение трехмерной модели лица

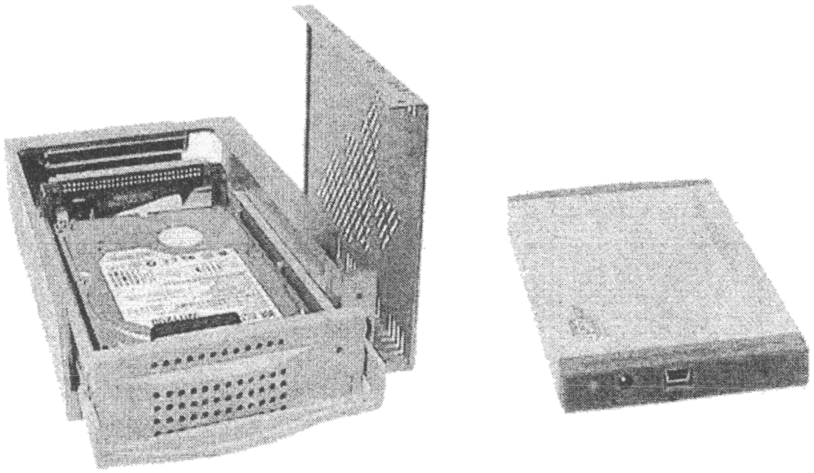

Рисунок 4 – Размещение жесткого диска на шасси типа Mobile Rack

Однако такой подход совершенно неприемлем в том случае, если компьютер является многопользовательской машиной, либо по каким-либо причинам доступ к данному компьютеру по сети должен быть круглосуточным. В этом случае, с одной стороны, необходимо решить задачу разграничения доступа пользователей, с другой – обеспечить беспрепятственный доступ легитимных пользователей. Естественно, что решение этих задач предусмотрено во всех современных операционных системах. Но, в виду того, что разграничение доступа к данным в современных ОС базируется на дискреционной политике безопасности, которая позволяет достаточно гибко осуществлять разграничение прав на доступ при, к сожалению, возможности формирования программными методами скрытых каналов утечки информации, в том числе, путем внедрения программного кода типа «троянский конь». Основным недостатком систем, основанных на дискреционной политике безопасности, является то, что механизмы безопасности, реализованные в этих системах, не позволяют контролировать потоки информации, циркулирующими между объектами информационной системы.

Контролировать потоки информации возможно в компьютерных системах, в основе которых лежит мандатная политика безопасности. Для реализации такой политики безопасности требуются дополнительные программные, аппаратные или программно-аппаратные механизмы. Последние два варианта являются достаточно дорогостоящими и применяются в случаях, когда речь идет о защите данных, содержащих дорогостоящие, либо государственные секреты, когда затраты на реализацию системы защиты адекватны стоимости защищаемой информации. Однако чисто программные средства с небольшими дополнениями аппаратного обеспечения позволяют реализовать защиту на доступ к приватным данным путем сравнительно небольших финансовых затрат.

Во-первых, требуется установить дополнительное программное обеспечение поверх стандартной операционной системы, позволяющее реализовывать мандатную политику безопасности. Спектр такого программного обеспечения достаточно широк. Наиболее известными программными продуктами такого рода являются «Страж NT» (рисунок 5), «Dallas Lock» (рисунок 6).

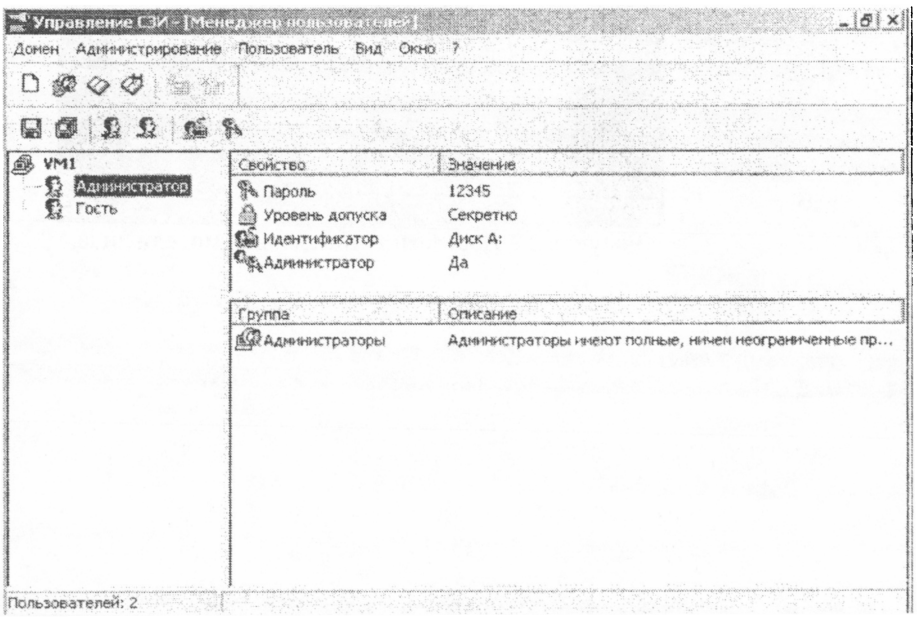

Рисунок 5 – Окно СЗИ «Страж-NT»

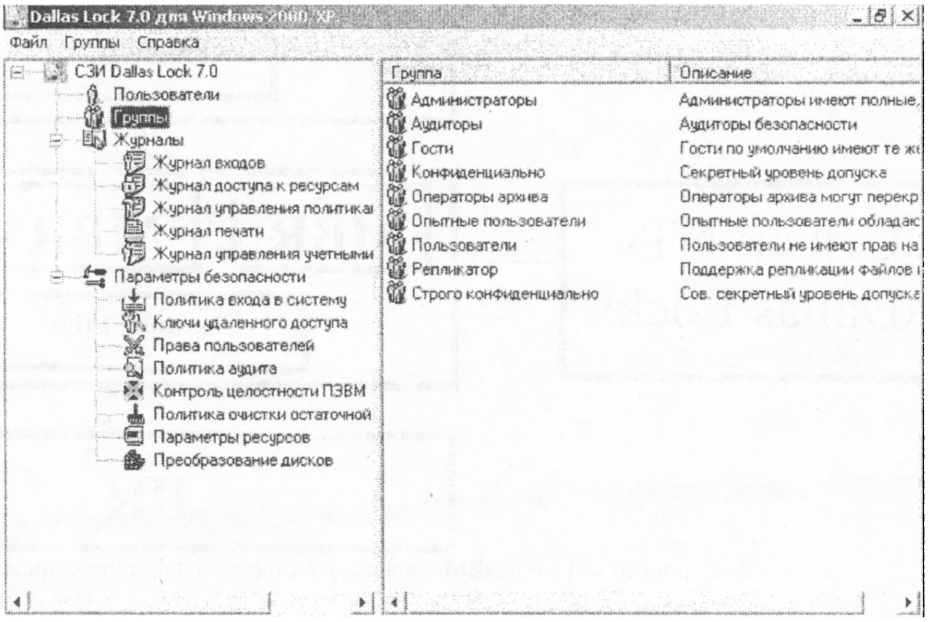

Рисунок 6 – Окно СЗИ «Dallas Lock»

Как правило, такого рода программы в процессе инсталляции осуществляют модернизацию MBR (Master Boot Record, главная загрузочная запись). Смысл такой модернизации заключается в следующем.

При стандартной загрузке ЭВМ осуществляется следующая последовательность действий. При включении питания управление ЭВМ берет на себя программа, записанная в постоянное запоминающее устройство (ПЗУ) ПК BIOS, которая производит процедуру самотестирования компьютера – Power-On Self-Test -- POST, после чего в оперативную память загружается содержимое первого сектора нулевого цилиндра нулевой стороны накопителя на жестком магнитном диске (НЖМД) (рисунок 7).

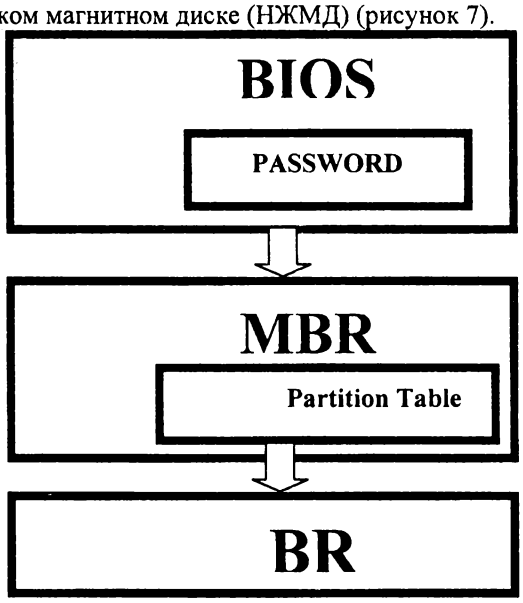

Рисунок 7 – Процесс загрузки ЭВМ при установленном пароле пользователя в BIOS

В данном секторе НЖМД находиться главная загрузочная запись MBR, которой передается управление компьютером. Программа первоначальной загрузки NSB (Non-System Bootstrap, несистемный загрузчик) является первой частью MBR. NSB анализирует таблицу разделов жесткого диска (Partition Table), являющуюся второй частью MBR, и определяет на ней расположение активного раздела НЖМД, содержащего рабочую версию операционной системы. Определив активный (загрузочный) раздел НЖМД, программа NSB считывает его нулевой сектор BR (Boot Record, загрузочная запись) и передает ей управление компьютером. Алгоритм работы загрузочной записи зависит от типа операционной системы, но обычно состоит в запуске самой операционной системы или программы – загрузчика операционной системы.

После инсталляции системы защиты информации (СЗИ), а, следовательно, модернизации MBR, алгоритм процедуры загрузки изменяется (рисунок 8).

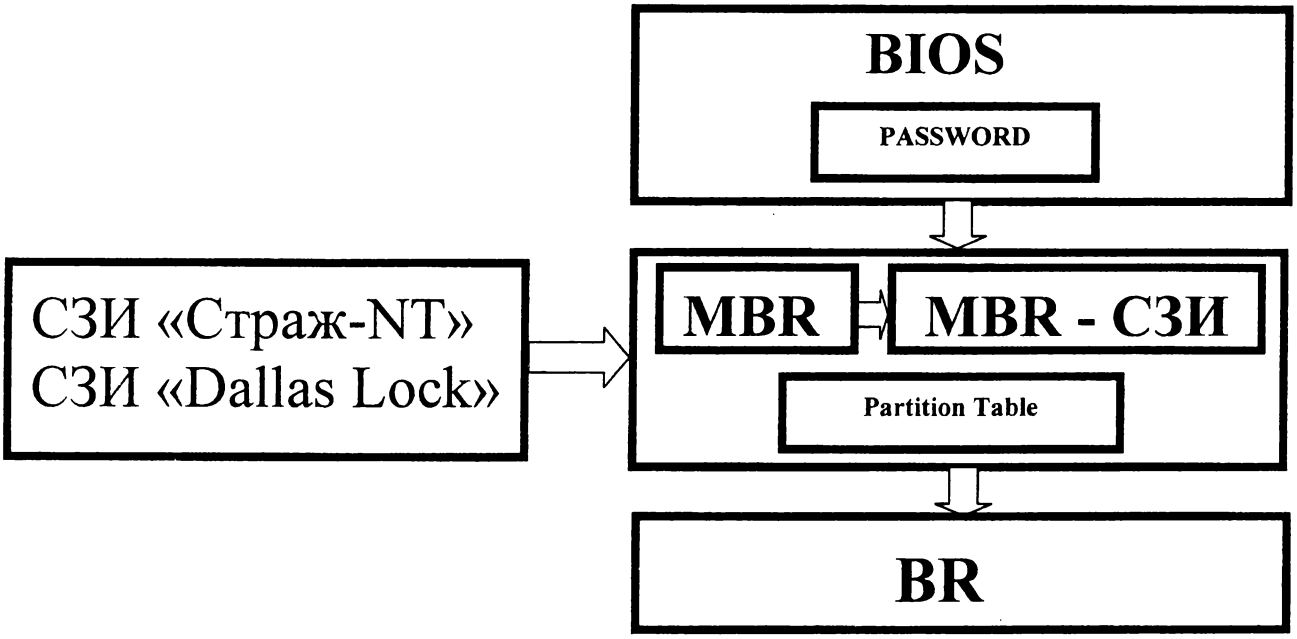

Рисунок 8 – Процесс загрузки ЭВМ с использованием модифицированной MBR

При обращении к модифицированной MBR – MBR-СЗИ – запускается программный код, ответственный за проведение процедур идентификации/аутентификации до начала загрузки операционной системы. Таким образом, защитные механизмы включаются до, а не в процессе загрузки операционной системы. По ходу этих процедур до ввода парольной информации СЗИ потребует предъявить идентификатор (рисунки 9,10), который, как правило, представляет собой физический носитель ключевой информации (рисунок 11).

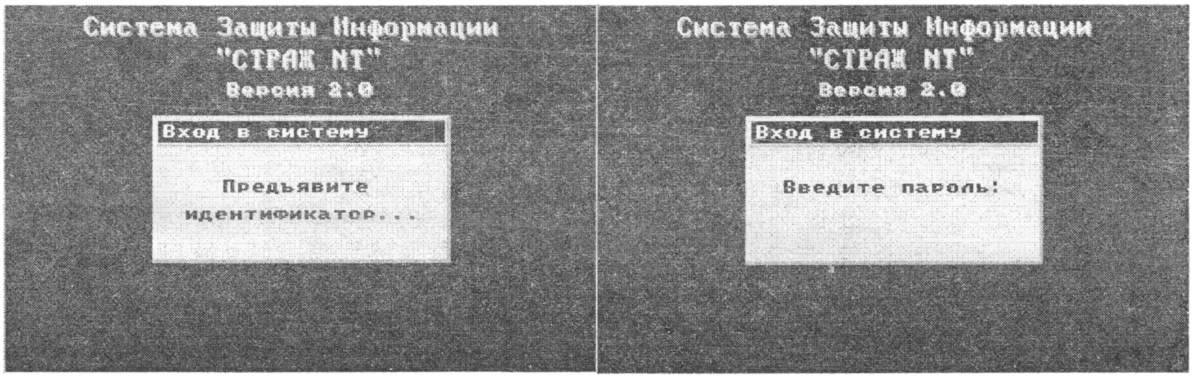

Рисунок 9 – Процесс входа в систему с установленным СЗИ «Страж NT»: а – запрос на предъявление идентификатора; б – запрос на ввод пароля

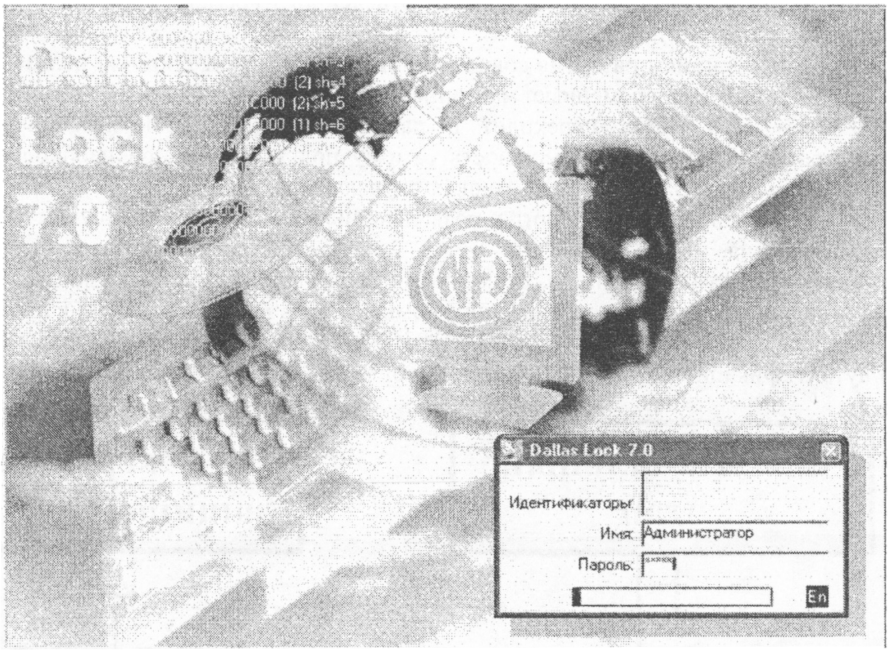

Рисунок 10 – Процесс входа в систему с установленным СЗИ «Dallas Lock»

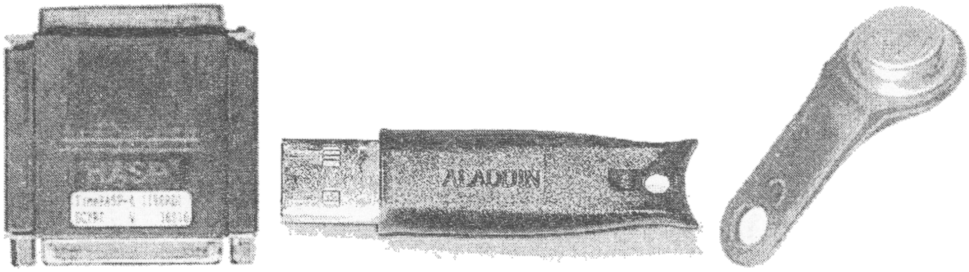

Рисунок 11 – Варианты исполнения носителей ключевой информации: а – носитель HAPS; в – носитель e-Token; б – носитель iButton

Как видно из рисунка 11, варианты носителей ключевой информации могут быть различны в зависимости от задействованного системой интерфейса. Некоторые из носителей ключевой информации (например, носитель iButton) требуют установки в компьютер дополнительной платы расширения (рисунок 12). Простейший же вариант – использование ключевой дискеты. Однако, учитывая тенденции развития современной компьютерной техники, можно констатировать, что данный тип носителя, являющийся практически единственным на протяжении многих лет, в настоящее время выходит из употребления в виду очень низкой надежности, и современные системные блоки в подавляющем случае не оборудуются приводами для работы с носителями этого типа.

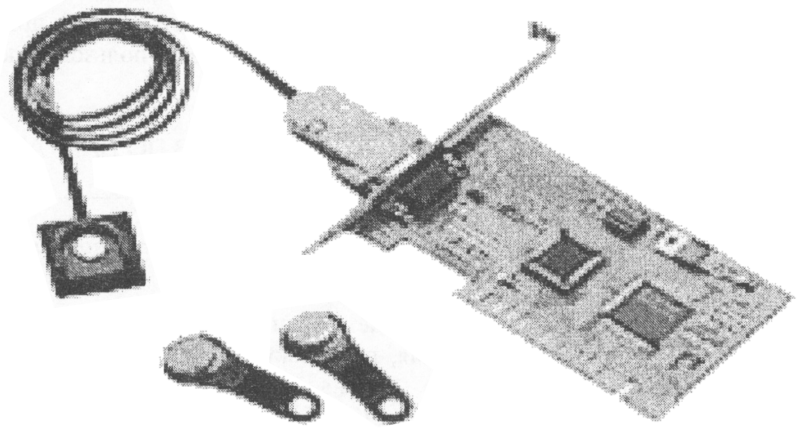

Рисунок 12 – Плата расширения для использования носителяключевой информации типа iButton

После предъявления идентификатора пользователь (при активированной функции) ограничен по времени и количеству попыток на ввод пароля, что позволяет свести к минимуму вероятность успешной атаки

на пароль методом прямого перебора. По истечении отведенного времени (исчерпании попыток ввода, как правило, 3 - 5) система потребует перезагрузки.

Возвращаясь к тенденциям развития современной компьютерной техники, нельзя не упомянуть такую особенность, как установка в современные материнские платы микросхем BIOS, выполненных по Flash-технологии. При этом ПЗУ BIOS переходит в разряд ППЗУ – перепрограммируемого постоянного запоминающего устройства. Это дает возможность самому пользователю при необходимости осуществлять перепрошивку содержимого BIOS, причем во многих случаях производители материнских плат поставляют в комплекте с ними специализированные утилиты, позволяющие такую прошивку осуществить непосредственно на компьютере пользователя.

Ориентируясь на такую тенденцию, пермская «Фирма НТЦ КАМИ» предложила использовать такую возможность для модернизации BIOS персонального компьютера в целях обеспечения процесса доверительной загрузки ОС. При этом устанавливаемая версия BIOS изначально требовала осуществления процедур идентификации/аутентификации до загрузки стационарной операционной системы (рисунок 13).

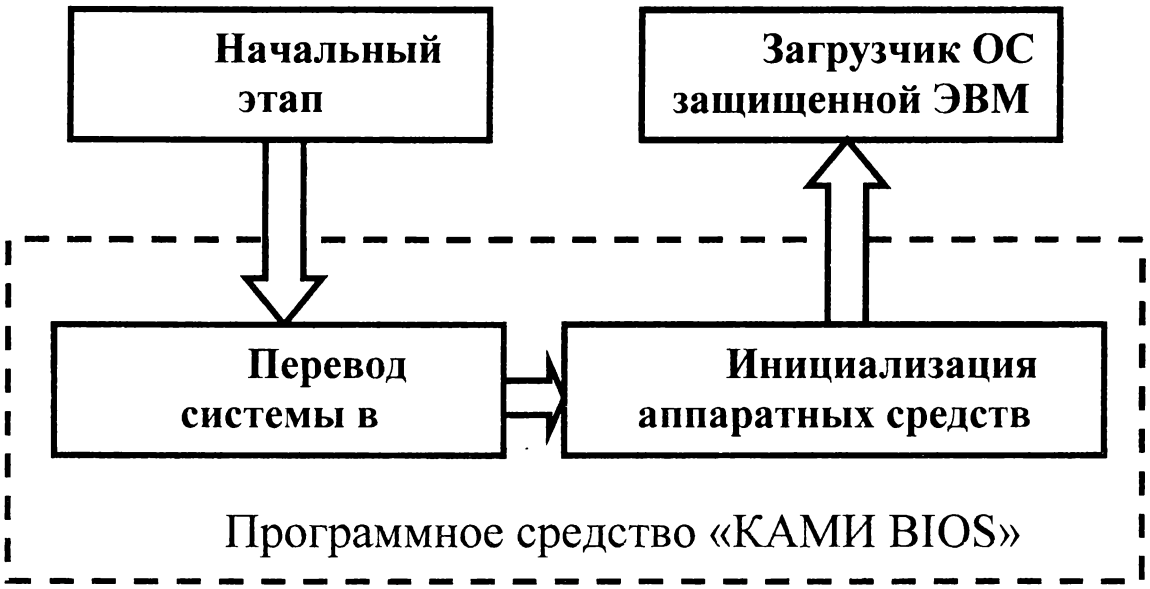

Рисунок 13 – Алгоритм работы программного средства (ПС) «КАМИ BIOS»

Такой подход имеет целый ряд преимуществ:

- простота реализации (программный код прошивается в микросхему BIOS);
- прозрачность программного кода (сертификация исходных текстов программ);
- невозможность обхода загрузки (без BIOS любая ЭВМ просто не загрузится).
- встраивание механизмов защиты (проведение контрольных процедур до загрузки ОС).

Таким образом, в настоящее время существует возможность защитить приватную информацию от НСД со стороны посторонних лиц посредством установки программных надстроек поверх стандартных операционных систем и модернизации BIOS. Такое решение позволяет, с одной стороны, многократно повысить устойчивость парольных систем от взлома. С другой стороны, подобные решения, хотя и являются менее надежными, чем системы, основанные на использовании биометрических признаков, имеют в гораздо меньшую стоимость и в связи с этим доступны к использованию рядовым пользователем.

Давыдова Е.М., Мещеряков Р.В., Шелупанов А.А.

КРИТИЧЕСКОЕ НАПРАВЛЕНИЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО НАПРАВЛЕНИЮ НАНОТЕХНОЛОГИЙ И НАНОЭЛЕКТРОНИКИ

office@keva.tusur.ru
Томский государственный университет систем управления и радиоэлектроники (ТУСУР)
г. Томск

В настоящее время в России активно развивается направление нанотехнологий и наноэлектроники, в частности. По мере развития данного направления, поскольку нанотехнология – междисциплинарная наука, потребуется множество специалистов разного уровня и направлений подготовки. Причем остаются актуальными вопросы подготовки специалистов в данной области. Формирование учебных программ в высшем учебном заведении сопряжено с рядом вопросов по их реализации. Особенно актуально это для специальностей инженерного профиля [1].

В ТУСУРе создано базовое подразделение «Центр нанотехнологий», которое координирует деятельность Вуза по направлению нанотехнологий и наноэлектроники. Очевидно, что учитывая специфику ТУСУРа в нем работы ведутся преимущественно в области наноэлектроники.