УДК 004.056.53

СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ ПО В КОМПЬЮТЕРАХ И СЕТЯХ ЭВМ ОТ НЕСАНКЦИОНИРОВАННОГО РАСПРОСТРАНЕНИЯ И КОПИРОВАНИЯ

А.И. Мартышкин[1], А.А. Воронцов[2]

[1]кандидат технических наук, доцент кафедры вычислительных машин и систем, ФГБОУ ВО «Пензенский государственный технологический университет», г. Пенза, Россия, e-mail: Alexey314@yandex.ru

[2]кандидат технических наук, доцент кафедры вычислительных машин и систем, ФГБОУ ВО «Пензенский государственный технологический университет», г. Пенза, Россия, e-mail: aleksander.vorontsov@gmail.com

Аннотация. В статье рассматриваются вопросы, связанные с существующими методами защиты ПО в компьютерах и сетях ЭВМ от несанкционированного копирования и распространения.

Ключевые слова: вычислительная система, защита информации, несанкционированный доступ, копирование, носитель информации, конфиденциальность.

MODERN METHODS OF SOFTWARE PROTECTION IN COMPUTERS AND COMPUTER NETWORKS FROM UNAUTHORIZED DISTRIBUTION AND COPYING

A.I. Martyshkin[1], A.A. Vorontsov

[1]Ph.D., Associate Professor of the Department of Computers and Systems, FGBOU VO "Penza State Technological University", Penza, Russia, e-mail: Alexey314@yandex.ru

[2]Ph.D., Associate Professor of the Department of Computers and Systems, FGBOU VO "Penza State Technological University", Penza, Russia, e-mail: aleksander.vorontsov@gmail.com

Abstract. The article deals with the issues related to the existing methods of software protection in computers and computer networks from unauthorized copying and distribution.

Keywords: computer system, information security, unauthorized access, copying, data carrier, confidentiality.

Введение. Одной из ведущих фирм в области компьютерных технологий и информационных вычислительных сетей является компания «International Business Machines» (IBM). Большое внимание фирма уделяет защите информации. Наиболее прогрессивные и перспективные достижения в этой области патентуются фирмой во всех государствах мира, развитых индустриально.

Цель работы. Рассмотреть методы защиты по в компьютерах и сетях ЭВМ от несанкционированного распространения и копирования

Материал и результаты исследований. К числу наиболее бурно развивающихся направлений за последние десятилетия можно отнести защиту программного обеспечения от несанкционированного использования и ограничение прав потребителя на использование покупаемого им программного обеспечения и/или на его размножение и копирование. В патенте [1] отмечается, что общепринятая стандартная архитектура вычислительных машин, в том числе ПЭВМ, является неэффективной с точки зрения защиты программного обеспечения (ПО) от несанкционированного использования и копирования (НСИиК). Предложена архитектура базовой защищенной вычислительной системы, важной компонентой которой, является дополнительный логически выделенный «физически» защищенный сопроцессор.

В этой системе ключ расшифрования ППО (АК) вводится и хранится в сопроцессоре (СП) с физически защищенного нетрадиционного носителя информации (НИ), который может быть сразу же после ввода уничтожен. Для того, чтобы пользователь мог запустить защищенное ПО, он должен ввести (инсталлировать) в ПЗУ сопроцессора «Право» в виде ключа пользователя АК. При этом СП вводит ключ АК вначале в ОЗУ, затем расшифровывает его на ключе супервизора CSK, проверяет его аутентичность путем взаимной верификации данных НИ с внешнего носителя с файлом $E_{AK}\left(T_1\right)$ методом вопрос/ответ и уничтожает данные на носителе T_1. После установления аутентичности и факта, что носитель T_1 не был использован, ключ АК переписывается в сопроцессоре в РПЗУ. Пользовательские файлы В вводятся в ОЗУ сопроцессора в зашифрованном виде на ключе АК. После расшифрования ППО исполняется в ОЗУ сопроцессора. Таким образом, в описываемой системе «Право» передается пользователю с помощью внешнего (нетрадиционного) НИ. Пока в памяти СП находится ключ АК пользователь может запускать на исполнение соответствующее защищенное ППО. При этом *никаких* ограничений «Права» для пользователя базовая система не предусматривает.

В 1992 г. фирмой IBM был запатентован метод «Управление правами пользователя программного обеспечения с защитой от копирования» [2]. Целью данного изобретения является: обеспечение безопасной передачи прав пользователям; ограничение прав пользователей.

При этом передача права может быть посредственной (с использованием промежуточного носителя) или непосредственной (сопроцессор/сопроцессор), а ограничение прав - по времени, по числу запусков ППО или по любому другому параметру. Возможность ограничения прав пользователей впервые дала продавцу ППО возможность проведения «политики

возврата», гарантирующей, что пользователь не оставил у себя работоспособной копии и не смог скопировать ПО.

Что касается второй цели, достигаемой этим изобретением, то следует отметить, что в защищенной системе предусмотрены следующие возможности: установка условия (ограничения) продавцом ПО; выбор критерия, по которому определяются ограничения; проверка выполнения условий по выбранному критерию программным способом.

Критерий выполняется программно и в засекреченном виде находится в составе файла ППО. Он не может быть прочитан и/или изменен со стороны пользователя (ЦП). С целью сохранения условий для проверки по критерию в РПЗУ сопроцессора выделена специальная область. В ней же находится ключ расшифрования ПО АК. Таким образом, пока существует «Право», существует «Условие». С целью, чтобы в качестве критерия могло выступать «Время» (например, ограничение права пользователя на запуск определенных файлов до 1.01.2002 г.) в состав СП введены часы, физически недоступные пользователю, с индивидуальным питанием. Для достижения удобства использования данной схемы защиты ПО, в системе предусмотрены следующие условия: так как «Право» существует в виде криптографического ключа в памяти СП, который может выйти из строя, то выход СП из строя не должен лишить пользователя «Права»; при выходе из строя СП никакой аппаратный метод не должен привести к генерации ложных прав пользователя.

Предложенный подход к решению проблем размножения и копирования ППО позволяет осуществлять передачу прав пользователя на определенный вид ПО между потребителями под контролем владельца программного продукта. Передача «Права» может осуществляется с помощью стандартных магнитных и электронных носителей или непосредственно с компьютера на компьютер. При передаче прав посредством промежуточных носителей информации пользователь приобретает у владельца ППО или у его производителя так называемый «комплект передачи права». В его состав входят: внешний носитель информации T_2 и диск (стандартный носитель информации) с файлом для передачи права. Этот файл является функцией зашифрования данных аутентификации на ключе супервизора: $E_{CSK}(T_2)$. Кроме того, для передачи права пользователю потребуется свой пользовательский стандартный диск (носитель информации). Следует обратить внимание на следующий факт. Передача права таким образом естественно гарантирует безопасность для владельца ППО, но возможна только при следующих условиях: терминал, на который передается ППО должен иметь свой СП со своим ключом супервизора CSK; передача прав возможна только между теми терминалами, которые имеют одинаковые ключи CSK;

если ключи CSK между двумя терминалами различны, то передача прав возможна только через супервизор, который имеет информацию о ключах CSK различных терминалов. При передаче прав непосредственно с компьютера на компьютер передаются только данные АК с соответствующими флагами и условиями, засекреченные на ключе супервизора: $E_{CSK}(AK, C)$. Все остальное ППО передается стандартными информационными средствами, в том числе и по почте.

Таким образом, политика «возврата» согласно описываемой системе защиты информации, заключается в следующем. Продавец (владелец) ППО ограничивает права пользователя (покупателя), например, временем гарантии. В конце срока Пользователь готовит «комплект передачи права» и возвращает его Продавцу. При этом ключ АК из памяти сопроцессора удаляется, остается только кратковременный ключ. Продавец путем анализа «Комплекта…» может убедиться в том, что у пользователя не осталось ПО. Комплект восстановления прав Продавец продает пользователю за отдельную плату. Основной задачей, которую ставила перед собой компания IBM перед созданием описанной выше системы защиты ПО от несанкционированного размножения и копирования, являлось сохранение функций передачи и распространения ПО стандартными средствами и общепринятыми носителями информации. Эта цель была достигнута ценой введения в вычислительные терминалы изолированной и физически защищенной аппаратной среды, представляющей собой независимые микро-ЭВМ, а также ценой наличия некоторого нестандартного, физически защищенного, носителя информации, сопутствующего стандартным пакетам ППО на обычных носителях и осуществляющего их аутентификацию.

Рассмотрим другой, диаметрально противоположный подход, к проблеме защиты ПО в вычислительных сетях и системах, предложенный фирмой «Kelly Services» [3]. Общей идеей, лежащей в основе двух систем, является признание факта, что для обеспечения определенного уровня надежной защиты ПО в ЭВМ (ПЭВМ) необходимо усовершенствование аппаратных средств и использование методов криптографии. Стандартная конфигурация ПЭВМ защиты ПО от НСД и НСК обеспечить не может.

В качестве обоснования своего оригинального подхода к проблемам защиты информации компания приводит следующие доводы. Согласно стандартной структуре вычислительных систем в настоящее время выделяют две среды хранения информации: жесткий диск (ЖД) и внешние носители информации, как электронные, так и магнитные. Любые данные, в том числе и конфиденциальные, могут быть легко скопированы с ЖД на внешние носители и выведены за пределы системы. При этом, если форматы и организация данных на внешних носителях являются стандартными, то этот

факт представляет серьезную угрозу для конфиденциальной информации. Если форматы и организация данных на внешних носителях являются уникальными, то это создает условия для обеспечения определенного уровня защиты. Первые попытки, предпринятые в этом направлении, были нацелены на использование принципа несовместимости вычислительных систем. Практическая реализация данного подхода привела к созданию неоперативных и ненадежных систем обработки информации. Частично эта проблема была отнесена на счет отсутствия каких-либо стандартов по взаимодействию пользовательского ПО с операционной системой (ОС), которая создает условия для его функционирования. Дело в том, что ППО должно быть подготовлено таким образом, чтобы функционирование ОС было прозрачно для пользователей. Поэтому, следование принципов несовместимости вычислительных систем привело к нарушению интерфейса с ОС. Возникли проблемы совместимости ППО с ОС.

Как результат, фирмой «Kelly Services» были выработаны следующие требования к разрабатываемой системе защиты информации. 1. Система защиты должна обеспечивать совместимость ОС и ППО с тем, чтобы служебные функции были прозрачны для пользователей. 2. Защищенная система должна работать как в сетях, так и как одиночный объект.

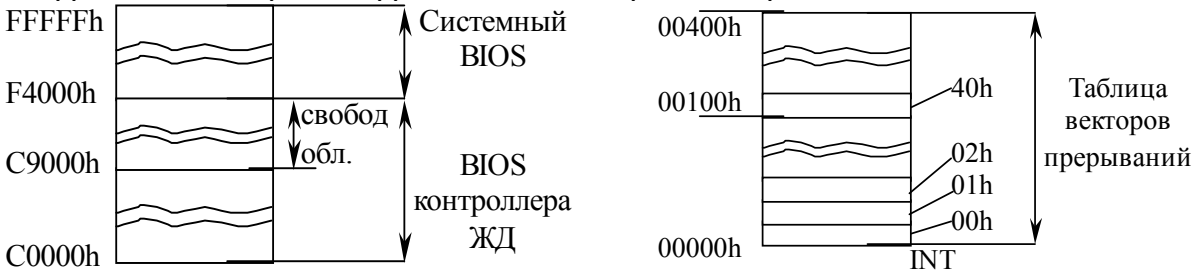
Следуя этим требованиям, компания предпочла сохранить полностью интерфейс DOS, а в вычислительную систему защиты вводить на самом низком уровне, в BIOS, подразумевая наличие специальных аппаратных средств. Структурная схема системы защиты программного обеспечения от НСД и НСК, используемая компанией «Kelly Services» приведена на рисунке 1.

Рисунок 1 - Структурная схема системы защиты программного обеспечения от НСД и НСК

В этой архитектуре система защиты представлена в виде секретной программы, располагаемой в области загрузочных адресов процессора. Она запускается на уровне BIOS и может обрабатывать данные, циркулирующие по крайней мере между одним из ГМД или ЖД. При этом данные становятся для процессора нечитаемыми. При защите данных, имеющих фай-

ловую организацию, FAT – таблица (File Allocation Table) также засекречивается, нарушая однозначную связь между отдельными файлами и их расположением в среде накопителей.

Рассмотрим пример функционирования данной системы защиты более подробно. Предположим, имеется ПЭВМ типа IBM PC/XT, как наиболее простая по архитектуре, на которой установлена PC-DOS или MS-DOS, хотя это условие не является принципиальным. Рассматриваемая система защиты использует область памяти РПЗУ BIOS в адресах $C9000h - F4000h$, зарезервированную для контроллера ЖД и являющуюся фактически свободной . Карта памяти представлена на рисунках 2, а и 2, б. Таблица векторов прерываний, согласно приведенного рисунка, содержит последовательность адресов в виде (сегмент: смещение), которые указывают процессору, в каких адресах находится программа обработки данного прерывания. Поскольку таблица векторов располагается в ОЗУ, то адреса в ней могут быть легко заменены. Этот факт используется таким образом, что адрес вектора прерывания $40h$, находящийся в области РПЗУ системного BIOS подменяется другим, начиная с которого в области BIOS в адресах $C9000h - F4000h$ расположены коды программы обращения к ГМД посредством расшифрования/зашифрования данных. Например, для IBM PC/XT адрес сегмента пишется в ячейку памяти 00102h, а смещение – в ячейку 00100h. При этом замена вектора прерывания происходит автоматически, в течении процесса тестирования аппаратных средств (POST), когда пользователь не может вмешаться в процесс инсталляции, на самом низком уровне BIOS. Этим гарантируется, что данные поступающие в/из ГМД будут автоматически зашифровываться/расшифровываться в процессе работы.



(область адресов $C0000h \div FFFFFh$) (область адресов $00000h \div 00400h$)

а *б*

Рисунок 2 – Карта распределения памяти

Алгоритм программы обработки INT 40h с процедурами защиты приведен на рисунке 3. Здесь знаком (*) отмечены процедуры, которые гарантируют, что последующее возможное обращение ЦП к области ОЗУ, где расположен буфер, не приведет к «зависанию» из-за того, что данные будут зашифрованы. Следует заметить, что, как правило, для подобных процедур

используют простые, но очень эффективные технологии, изменяющие порядок бит путем их циклического сдвига. Эти процедуры выполняются в регистрах ЦП и осуществляются очень быстро с использованием цепных команд. Для этого требуется только указать ЦП адрес начала и объем массива (буфера).

Рассмотренный подход к организации системы защиты данных ПЭВМ обеспечивает засекречивание и защиту не только ППО, но и таблицы FAT, а также указателей директорий. Для стандартных операционных систем, в том числе, для DOS, защищенная дискета полностью нечитаема. На ней даже имена файлов представлены в защищенном виде. Ценой защиты данных ПЭВМ является факт, что компьютер не может производить операции со стандартными дискетами в полном объеме: внешние носители несовместимы.

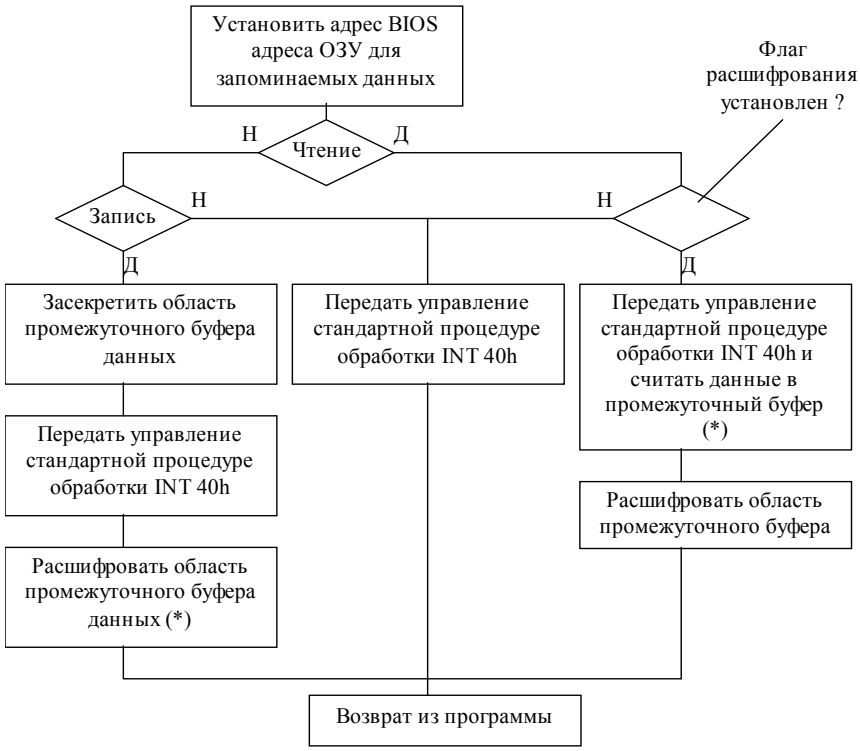


Рисунок 3 - Алгоритм программы обработки INT 40h с процедурами защиты

Мы проанализировали два наиболее характерных для настоящего времени подхода к проблеме защиты данных в терминальных ПЭВМ от несанкционированного копирования. И те, и другие принципы широко применяются на практике, однако, отражают два противоположных направления. Первый из них основан на полном сохранении всех стандартных внешних интерфейсов и совместимости со средствами вычислительной техники, в том числе, на сетевом уровне. При втором подходе гарантией невозмож-

ности несанкционированного копирования является несовместимость защищенного терминала по всем стандартным интерфейсам внешнего обмена. Первый метод требует значительно больших затрат, так как он связан с установкой дополнительных периферийных узлов, но, очевидно, обеспечивает защиту даже при доступе злоумышленника к аппаратным средствам. Второй метод – боле дешевый и может быть реализован программным способом. Защиту данных при доступе злоумышленника к аппаратным средствам он не обеспечивает.

Вывод. Конкретные рекомендации по использованию того или иного метода защиты программ и данных от несанкционированного копирования могут быть продиктованы лишь с учетом заданных условий пользователя, а также рассматриваемых в статье недостатков и положительных сторон того и другого.

ЛИТЕРАТУРА

1. Hardware protection against software piracy – The communications of the ASM, v27, no.9, 1984.
2. Manipulating rights-to execute in connection with a software copy protection mechanism – US patent, no5,109,413.
3. Computer software encryption apparatus. US patent, no 4,937,861.

УДК 004.94; 167.7

ЗАСОБИ ВІЗУАЛІЗАЦІЇ В НАУЦІ ТА ОСВІТІ

Г.С. Тен[1], О.М. Твердохліб[2], І.В. Вернер[3]
[1,2,3]асистент кафедри основ конструювання механізмів і машин, Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна, e-mail: ill3@ukr.net

Анотація. У роботі проводиться огляд найбільш доступних і поширених систем візуалізації графічної інформації, а також аналізуються можливості їх використання.

Ключові слова: візуалізація, rendering, Autodesk, Adobe, освіта.

VISUALIZATION IN SCIENCE AND EDUCATION

Anna Ten[1], Alexander Tverdohleb[2], Ilya Verner[3]
[1,2,3]Assistant, Machinery Design Bases Department, National Miming University, Dnipro, Ukraine e-mail: ill3@ukr.net

Abstract. The most accessible and widely used visualization systems for graphic information are reviewed. The possibilities of it using are analyzed.