УДК 004.056.5

Е.А. Чаус[1]

ЗАЩИТА ИНФОРМАЦИИ НА ПОДКЛЮЧЕННОМ К ИНТЕРНЕТУ КОМПЬЮТЕРЕ

E.A. Chaus

DATA PROTECTION ON THE INTERNET-CONNECTED COMPUTER

В последнее время все более широкое применение находит электронная подпись (ЭП). Причем, зачастую она используется для подтверждения подлинности документов, передаваемых через Интернет. Для безопасного ее применения необходимо хранить в секрете закрытый ключ, используемый для выполнения ЭП. Для защищенного хранения ключей и сертификатов, а также защиты процесса выполнения ЭП используются USB-устройства производства компаний, среди которых наиболее известны: «Аладдин Р.Д.» (eToken) [1]; «Актив» (рутокен) [2]; ISBC (ESMART Token) [3], ООО Фирма «АНКАД» («Анкадер») [4], ОКБ САПР (ПСКЗИ ШИПКА) [5]. Большинство модификаций этих устройств выполняют следующие функции:

• формирование и проверку ЭП-данных по зарубежным и отечественным алгоритмам;

• вычисление хеш-функции;

• шифрование/расшифровывание данных;

• формирование в микросхеме ключей шифрования и электронной цифровой подписи (ЭЦП);

• хранение закрытого ключа для ЭЦП в защищенном от несанкционированного доступа (НСД) виде;

• хранение ключей шифрования в защищенном от НСД виде;

• безопасное хранение паролей и другой текстовой информации.

Кроме перечисленных характеристик устройства обладают некоторыми дополнительными характеристиками, приведенными в таблице 1.

Однако использование такого устройства не обеспечивает защиты от подписи посторонних документов в момент наличия в компьютере, подключенного к нему USB-устройства, с помощью заранее внедренных различным образом «вирусных» программ. Поэтому большое значе-

Таблица 1

Сравнительная таблица USB-устройств (Token)

Основные характеристики USB- устройств (Token)	eToken NG-FLASH	Рутокен ЭЦП Flash	ESMART Token	ПСКЗИ ШИП-КА-1.6	ПСКЗИ ШИП-КА-2.0	Анкадер
1. Физический датчик случайных чисел	–	–	Есть КСЗ	Есть КСЗ	–	Есть КСЗ
2. Дополнительная Flash-память	До 16 Гб	4ГБ	–	Data Flash по заказу – до 8 МВ	Data Flash 512 КВ	До 16 Гб
3. Доверенная загрузка операционной системы с USB-устройства	+	–	–	–	–	+
4. Наличие СКЗИ в виде отечественной микро-схемы	–	–	+	–	–	+

[1] Ассистент кафедры прикладной информатики Ступинского филиала АНО ВО «Российский новый университет».

ние при использовании этих устройств является обеспечение их работы в доверенной операционной системе (ОС). Предлагаются два варианта защиты компьютера от НСД в сети Интернет.

В первом варианте предлагается использовать две ОС: доверенную, размещенную во флеш-памяти USB-устройства, для работы с закрытой информацией без выхода в Интернет, и обычную ОС компьютера для выхода в Интернет. Переход из одной ОС в другую осуществляется путем перезагрузки. Причем, первым устройством для загрузки ОС в BIOS компьютера рекомендуется поставить USB-носитель.

При этом флеш-память устройства может также использоваться для переноса информации между открытой и закрытой системами. Например, мы выполняем загрузку ключей в устройство, подпись документов, шифрование в доверенной среде. Результаты записываем на ту же флеш-память, с которой загружались, или на другой USB-носитель. Далее перезагружаем компьютер, подключаем USB-носитель с обработанными документами и пересылаем их по Интернету в зашифрованном или открытом виде с подписью. Также поступаем и при работе в сети Интернет: полученную из Интернета информацию переносим в закрытую систему на том же USB-носителе.

Данный вариант обеспечивает требуемую степень защиты данных для домашних компьютеров и отдельных компьютеров предприятия. Для доверенной загрузки в этом варианте можно использовать обычные или защищенные USB-носители с дополнительной Flash-памятью (например, eToken NG-FLASH [1], «Анкадер [4]). Для других USB-носителей, приведенных в таблице 1, рекомендуется дополнительно использовать доверенную ОС, размещенную на обычной USB-Flash, либо поддерживать доверенную среду на жестком диске компьютера. Для обычного USB-Flash носителя защита информации обеспечивается использованием переключателя защиты от записи и шифрованием. Основные механизмы реализуются программным способом с поддержкой программной доверенной среды работы с данными.

Государственным учреждениям, для которых необходимо выполнять требования Указа Президента РФ № 351 от 17.03.2008 г. «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», и корпоративным пользователям предлагается альтернативное техническое решение по совмещению возможностей доступа и обработки разнокатегорийной информации на одном ПК.

Во втором решении предлагается загрузка доверенной ОС с жесткого диска для обработки корпоративной информации и загрузка открытой ОС для выхода в Интернет с внешнего загрузочного USB-носителя для работы в открытой сети. Аппаратное разделение ОС осуществляется аппаратно-программным модулем доверенной загрузки (АПМДЗ) [4], изображенным на рис. 1.

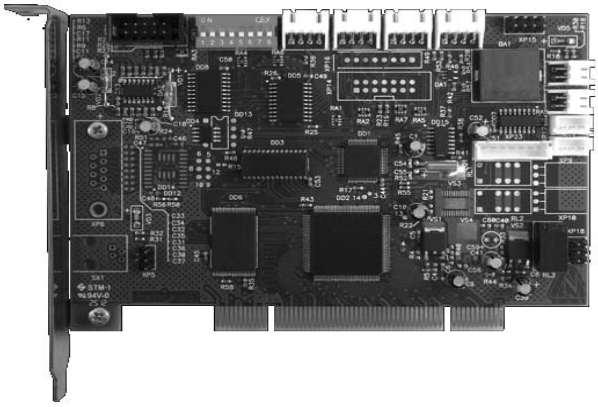

Рис. 1. АПМДЗ «КРИПТОН-ЗАМОК»

Для реализации второго варианта используются следующие аппаратные компоненты.

Аппаратные компоненты, устанавливаемые в системный блок компьютера:

– АПМДЗ – сертифицированное изделие М-526А;

– доверенный 2-канальный сетевой интерфейсный адаптер – AncNet x2 TX;

–- коммутатор питания жесткого диска с интерфейсом SATA.

Аутентифицирующие носители – touch memory (ТМ):

– ТМ № 1 – для обработки корпоративной информации на жестком диске (ЖД);

– ТМ № 2 – для работы в открытой сети.

Внешний загрузочный USB-носитель с ОС, оптимизированный для работы с флэш-памятью.

Администратор системы АПМДЗ производит настройку системы таким образом, чтобы пользователь с ТМ № 1 загружался с жесткого диска и имел доступ в корпоративную сеть, а с ТМ № 2 – загружался с внешнего USB-носителя и имел доступ в сеть Интернет.

После старта BIOS АПМДЗ перехватывает управление, производит идентификацию и аутентификацию пользователя (пользователь предъявляет свой экземпляр ТМ-идентификатора и вводит пароль), после чего АПМДЗ в зависимости

от идентификатора пользователя выдает сигналы управления 2-канальному сетевому адаптеру и коммутатору жесткого диска и затем передает управление на загрузку ОС либо с жесткого диска, либо с внешнего USB-носителя.

Таблица 2

Варианты загрузки ОС

ТМ	Контур	Аппаратная конфигурация компьютера	Источник загрузки ОС
№ 1	Корпоративный	ЖД, 1-й канал СИА (рис. 2) USB	ЖД
№ 2	Открытый Интернет	2-й канал СИА USB	Внешний USB-носитель

В случае если предъявленный ТМ не зарегистрирован в системе или несколько раз неправильно введен пароль, компьютер блокируется.

Таким образом, при предъявлении АПМДЗ носителя ТМ № 1 для работы в корпоративной сети после идентификации и аутентификации пользователя происходит:

• блокировка выхода AncNet x 2 TX в открытую сеть;

• подключение жесткого диска для работы в корпоративной сети через коммутатор питания жесткого диска;

• включение выхода AncNet x 2 TX в корпоративную сеть;

• загрузка операционной системы с жесткого диска.

При предъявлении в АПМДЗ носителя ТМ № 2 для работы в открытой сети после идентификации и аутентификации пользователя происходит:

• блокировка жесткого диска для работы в корпоративной сети через коммутатор питания жесткого диска;

• блокировка выхода AncNet x2 TX в корпоративную сеть;

• включение выхода AncNet x2 TX в открытую сеть;

• загрузка операционной системы с внешнего USB-носителя.

Таким образом, использование платы управления АПМДЗ позволяет осуществлять контроль целостности файлов на жестком диске.

Обмен информации происходит следующим образом: при работе в сети Интернет скачиваемая информация сохраняется на внешнем USB-носителе, при загрузке с жесткого диска возможность работы с внешним USB-носителем сохраняется, поэтому пользователь сможет уверенно использовать информацию из сети Интернет.

АПМДЗ «КРИПТОН-ЗАМОК» [4] предназначен:

• для разграничения и контроля доступа к техническим, программным и информационным ресурсам компьютера;

• для контроля целостности установленной на компьютере программной среды при запуске компьютера.

Устройство «КРИПТОН-ЗАМОК» может использоваться как для защиты конфиденциальной информации, так и для защиты информации, составляющей государственную тайну, что позволяет использовать его и для надежной защиты корпоративной информации ограниченного распространения.

В состав основных реализуемых функций устройства входят следующие:

• регистрация пользователей и запись аутентифицирующей информации пользователя на ключевой носитель;

• идентификация и аутентификация пользователя при запуске компьютера;

• регистрация событий доступа к компьютеру в электронном журнале;

• блокировка запуска компьютера при НСД;

• контроль целостности загружаемой ОС;

• аппаратная защита от несанкционированной загрузки ОС с гибкого диска, CD/DVD-ROM (при использовании соответствующих аппаратных коммутаторов);

• управление запуском устройств шифрования «КРИПТОН-4S/PCI», «КРИПТОН-8S/PCI» [4] в зависимости от прав входящего пользователя;

• управление доступом к накопителям жестких и гибких дисков (при использовании соответствующих аппаратных коммутаторов), к сетевым картам;

• управление порядком загрузки ОС с жестких дисков;

• звуковая сигнализация о состоянии изделия и событий доступа;

• управление блокировкой открытия корпуса компьютера;

• защита компьютера при нештатном электрическом воздействии на тракт ввода ключевой информации;

• инициализация дополнительных модулей защиты информации шифраторов сетевого трафика КСИА, шифраторов информации на жестком диске ПШД/IDE, ПШД/SATA, ПШФД/USB [4].

Разграничение доступа пользователей к аппаратным ресурсам рабочего места и управление загрузкой компьютера осуществляется на основе настройки администратора индивидуальных параметров каждого пользователя.

Разграничение доступа к аппаратным ресурсам со стороны прикладного ПО пользователя осуществляется после загрузки ОС. При помощи ПО можно получить набор прав из следующего списка:

- читать с ключевого носителя;
- писать на ключевой носитель;
- читать журнал;
- удалять записи из журнала
- читать из ОЗУ АПМДЗ;
- писать в ОЗУ АПМДЗ;
- читать с ГМД;
- писать на ГМД;
- осуществлять мягкий режим контроля целостности.

АПМДЗ имеет возможность управления блокировкой работы двух сетевых интерфейсных адаптеров типа AncNet Pro или двумя каналами AncNet x 2. Для каждого пользователя системный администратор может установить индивидуальные варианты доступа к двум каналам сети Ethernet после загрузки ОС:

Сетевой интерфейсный адаптер “AncNet x 2” является результатом модернизации сетевого интерфейсного адаптера “AncNet Pro” с целью обеспечения возможности выполнения управляемой работы с двумя каналами сети Ethernet. Данное изделие предназначено для обеспечения приема/передачи данных между ПК и двумя каналами сетевого оборудования (линии связи, концентраторы, переключатели, мосты и т.д.), составляющим информационную сетевую среду с типом доступа CSMA/CD и стандартом физического уровня 100Base-TX, 100Base-FX, 10Base-T. Внешний вид устройства показан на рис. 2.

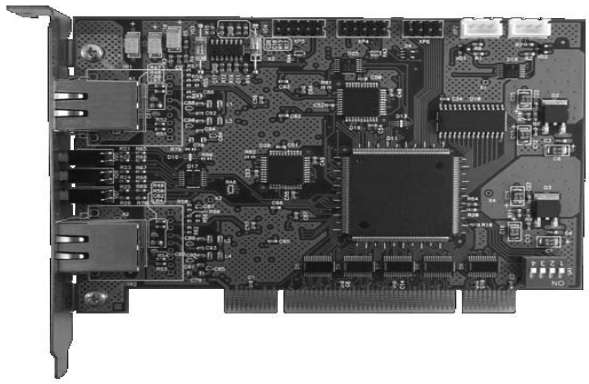

Рис. 2. Сетевой интерфейсный адаптер “AncNet x 2”

Во втором варианте получаем универсальное защищенное многопользовательское рабочее место. Оно позволяет осуществлять защиту информации в корпоративной сети и осуществлять доступ к сети Интернет.

Таким образом, в настоящее время можно с помощью предложенных средств организовать одно рабочее место для работы с информацией, предоставляющей тайну, и для выхода в сеть Интернет.

Литература

1. Материалы сайта http://www.aladdin-rd.ru/
2. Материалы сайта http://www.rutoken.ru/products/all/
3. Материалы сайта http://www.esmart.ru/product/esmart-token-gost/
4. Материалы сайта http://www.ancud.ru/
5. Материалы сайта http://www.okbsapr.ru/