УДК 621.3.019.3

Н.В. СЕСПЕДЕС ГАРСИЯ*

О КОНТРОЛЕ СОБЛЮДЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

*Институт проблем математических машин и систем НАН Украины, Киев, Украина

Анотація. *У статті розглянуто методи контролю дотримання конфіденційності комп'ютерних систем. Описано найбільш актуальні і широко використовувані засоби, а саме програмно-апаратні, організаційні і змішані засоби захисту. У питаннях більш серйозного захисту від несанкціонованого доступу більший інтерес представляють спеціальні засоби захисту.*
Ключові слова: *конфіденційність, захист від несанкціонованого доступу, програмні засоби захисту, апаратні засоби захисту, змішані засоби захисту, спеціальні засоби захисту.*

Аннотация. *В статье рассмотрены методы контроля соблюдения конфиденциальности компьютерных систем. Описаны наиболее актуальные и широко используемые средства, а именно программно-аппаратные, организационные и смешанные средства защиты. В вопросах более серьезной защиты от несанкционированного доступа больший интерес представляют специальные средства защиты.*
Ключевые слова: *конфиденциальность, защита от несанкционированного доступа, программные средства защиты, аппаратные средства защиты, смешанные средства защиты, специальные средства защиты.*

Abstract. *The methods to control the confidentiality of computer systems were considered in article. The most relevant and widely used tools, namely hardware and software, organizational and mixed protection tools were described. In matters of more serious protection against unauthorized access are more interested in special protection tools.*
Keywords: *confidentiality, protection against unauthorized access, software protection tools, hardware protection tools, mixed protection tools, special protection tools.*

1. Введение

Повсеместное использование и освоение информационных технологий наряду с позитивным влиянием на жизнедеятельность человека вызывают еще и ряд дополнительных проблем. Одной их серьезных проблем является проблема несанкционированного проникновения в компьютер или в компьютерные системы (КС) и сети посторонних лиц. Встречаются ситуации, когда даже обычный школьник может «взломать» сервер серьезной компании или организации, что приводит к частичной остановке работы и/или серьезным материальным потерям. Также существует определенная доля опасности нарушения конфиденциальности при автоматическом обновлении программного обеспечения и антивирусных программ, особенно это касается пиратских версий программ. Поэтому специалистам компьютерной техники необходимо решать ряд серьезных вопросов по созданию защиты компьютеров от несанкционированного проникновения. Необходимо создавать программные продукты, которые могли бы выявлять проникновение посторонних пользователей и блокировать доступ к компьютеру.

Несанкционированный доступ (НСД) постороннего лица в компьютер опасен не только возможностью прочтения и/или модификации электронных документов, но и возможностью внедрения им управляемой программы, которая позволит читать и/или модифицировать документы, хранящиеся на компьютере, осуществлять захват конфиденциальной информации (пароли и т.д.), осуществлять массовую рассылку спама с “захваченного” компьютера, удалять информацию на компьютере или вывести компьютер из строя, запус-

ISSN 1028-9763. Математичні машини і системи, 2015, № 3

тив вредоносное программное обеспечение. Это критично в тех отраслях, где нарушение конфиденциальности КС может привести, например, к человеческим жертвам.

Конфиденциальность КС – свойство системы обеспечивать защиту от несанкционированного использованияи информации или технического средства, подмены информации или технического средства, повреждения информации или технического средства со стороны внутреннего или внешнего агента.

Конфиденциальность КС обеспечивается программно-аппаратными, организационными и смешанными средствами защиты. Такие средства способствуют достижению более высоких показателей эффективности, если применять их комплексно.

2. Средства защиты информации

Средства защиты информации – это совокупность инженерно-технических, электрических, электронных, оптических и других устройств, приборов и технических систем, которые используются для решения различных задач по проблемам защиты информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы [1].

Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Одни средства препятствуют физическому проникновению, другие – препятствуют доступу к информации и данным. Первую часть задачи решают банальные дверные замки, решетки на окнах, защитная сигнализация и др. Вторую – технические средства защиты информации в компьютерах (экранирование), генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств – это надежность, независимость от субъективных факторов, высокая устойчивость к модификации. Недостатки – относительно большие объем и масса, недостаточная гибкость, высокая стоимость.

Программные средства включают программы для идентификации и аутентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, антивирусные программы, программы тестового контроля системы защиты, средства архивации данных, криптографические средства, средства управления доступом, протоколирование, аудит и др. Преимущества программных средств – универсальность, надежность, гибкость, простота установки, способность к модификации и развитию. Недостатки – ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Смешанные аппаратно-программные средства реализуют те же функции, что и аппаратные и программные средства в отдельности, и имеют промежуточные свойства.

Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки – высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

Наиболее распространенными, доступными и удобными являются программные средства. Другие средства используются в случаях необходимости обеспечения дополнительного уровня защиты информации или технических средств.

3. Аппаратные средства защиты информации

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства, позволяющие обеспечить защиту от сбоев в электропитании, от сбоев серверов, рабочих станций, компьютеров, устройств хранения информации и т.д. К настоящему времени разработано значительное число аппаратных средств различного назначения, однако наибольшее распространение получают следующие [1]:

• специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;

• устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;

• схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.

• устройства для шифрования информации (криптографические методы).

Для защиты периметра информационной системы создаются [1]:

• системы охранной сигнализации;

• системы цифрового видеонаблюдения;

• системы контроля и управления доступом (СКУД).

Защита информации от ее утечки техническими каналами связи обеспечивается следующими средствами и мероприятиями [1]:

• использованием экранированного кабеля и прокладкой проводов и кабелей в экранированных конструкциях;

• установкой на линиях связи высокочастотных фильтров;

• построением экранированных помещений;

• использованием экранированного оборудования;

• установкой активных систем зашумления;

• созданием контролируемых зон.

4. Программные средства защиты информации

Программные средства защиты включают программы для идентификации и аутентификации пользователей, антивирусные программы, средства управления доступом, средства шифрования информации, криптографические средства, средства архивации данных и др.

Антивирусная программа (антивирус) – программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом.

Ниже приведен список антивирусных программ с указанием страны происхождения [1]:

• AhnLab – Южная Корея;

• ALWIL Software (avast!) – Чехия (бесплатная и платная версии);

• AOL Virus Protection в составе AOL Safety and Security Center (Польша);

• ArcaVir – Польша;

• Authentium – Великобритания;

• AVG (GriSoft) – Чехия (бесплатная и платная версии, включая файрвол);

• Avira – Германия (есть бесплатная версия Classic);

• AVZ – Россия (бесплатная); отсутствует real-time monitor;

• BitDefender – Румыния;
• BullGuard – Дания;
• ClamAV – лицензия GPL (бесплатная, с открытым исходным кодом), отсутствует real-time monitor;
• ClamWin – ClamAV для Windows;
• Comodo Group – США;
• Computer Associates – США;
• Dr.Web – Россия;
• Eset NOD32 – Словакия;
• Fortinet – США;
• Frisk Software – Исландия;
• F-PROT – Исландия;
• F-Secure – Финляндия (многодвижковый продукт);
• G-DATA – Германия (многодвижковый продукт);
• GeCAD – Румыния (компания куплена Microsoft в 2003 году);
• GFI Software – Чехия;
• IKARUS – Австрия;
• H+BEDV – Германия;
• Hauri – Южная Корея;
• McAfee – США;
• Microsoft Security Essentials – бесплатный антивирус от Microsoft , США;
• MicroWorld Technologies – Индия;
• MKS – Польша;
• MoonSecure – лицензия GPL (бесплатная, с открытым исходным кодом), основан на коде ClamAV, но есть real-time монитор;
• Norman – Норвегия;
• NuWave Software – Украина (используют движки от AVG, Frisk, Lavasoft, Norman, Sunbelt);
• Outpost – Россия (используются два antimalware движка: антивирусный от компании VirusBuster и антишпионский, бывший Tauscan, собственной разработки);
• Panda Software – Испания;
• Quick Heal AntiVirus – Индия;
• Rising – Китай;
• ROSE SWE – Германия;
• Safe`n`Sec – Россия;
• Simple Antivirus – Украина;
• Sophos – Великобритания
• Spyware Doctor – антивирусная утилита;
• Symantec – США;
• Trend Micro – Япония (номинально Тайвань/США);
• Trojan Hunter – антивирусная утилита;
• Universal Anti Virus – Украина (бесплатный);
• VirusBuster – Венгрия;
• ZoneAlarm AntiVirus – США
• Zillya! – Украина (бесплатный);
• Антивирус Касперского – Россия;
• ВирусБлокАда (VBA32) – Беларусь;
• Dr. Solomon's Anti-Virus Toolkit – США;
• Украинский национальный антивирус – Украина.

Кроме вышесказанного, существуют много других доступных средств контроля соблюдения конфиденциальности в компьютерных системах, а именно [2]:

MyLanViewer – программа для многопоточного (для ускорения) сканирования и мониторинга компьютеров в сети с возможностью поиска общедоступных файлов;

GlassWire – программа представляет собой инструмент сетевого мониторинга со встроенным фаерволом;

USB Blocker – NetWrix USB Blocker – инструмент, обеспечивающий централизованный контроль доступа, предотвращая несанкционированное использование сменных носителей, подключаемых к USB-портам компьютера (карты памяти, внешние жесткие диски, устройства iPod и др.);

Leak Blocker – инструмент, предотвращающий утечку данных с корпоративных компьютеров через съемные устройства;

Lan Work – программа для мониторинга и управления соединениями, позволяющая просматривать активные подключения, открытые на компьютере через сеть файлы и следить за трафиком;

WebWatchBot -программа для анализа и мониторинга сети;

ShareWatcher – контролирует сетевые общедоступные ресурсы и разрешения на папки;

Alchemy Eye – программа для сетевого мониторинга, которая непрерывно следит за работоспособностью и состоянием серверов;

Net Tools – программа для сканирования Wi-Fi сетей и подключенных к ним устройств;

NetGong – программа автоматического отслеживания критических сбоев в работе большого числа серверов, маршрутизаторов, мостов и других устройств, находящихся в вашей сети;

TrafMeter – утилита, служащая для мониторинга входящего и исходящего интернет-трафика в режиме реального времени;

Microsoft Network Monitor – утилита для анализа сетевого трафика - позволяет захватывать сетевой трафик, просматривать и анализировать его;

Performance Monitoring Protocol – утилита, позволяющая осуществлять мониторинг в реальном времени работы нескольких серверов в целях обнаружения нестабильностей в работе удаленных ПК;

Remote Task Manager – программа для удаленного контроля и определения хода выполнения задач, процессов, сервисов, работы устройств, использования общих ресурсов в сетях LAN, WAN или через Интернет.

К программным средствам защиты информации также относятся специализированные средства защиты, которые в целом обладают лучшими возможностями и характеристиками, чем встроенные средства [3]:

Межсетевые экраны (также называемые брандмауэрами или файрволами, от нем. Brandmauer, англ. firewall – «противопожарная стена») – это специальные промежуточные серверы между локальной и глобальной сетями, которые инспектируют и фильтруют весь проходящий через них трафик в соответствии с заданными правилами. Межсетевые экраны позволяют резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняют эту опасность полностью. Более защищенная разновидность метода – это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой [1]. Существуют также и персональные межсетевые экраны, защищающие только компьютер, на котором они установлены. Межсетевые экраны также располагаются на периметре защищаемых сетей и фильтруют сетевой трафик согласно настроенной политике безопасности.

В табл. 1 приведены популярные межсетевые экраны:

Таблица 1. Межсетевые экраны

Межсетевые экраны	
Бесплатные	Ashampoo FireWall Free • Comodo • Core Force (англ.) • Online Armor • PC Tools • PeerGuardian (англ.) • Sygate (англ.) • ZoneAlarm
Проприетарные	Ashampoo FireWall Pro • AVG Internet Security • CA Personal Firewall • Jetico (англ.) • Kaspersky • Microsoft ISA Server • Norton • Outpost • Trend Micro (англ.) • Windows Firewall • Sunbelt (англ.) • WinRoute (англ.)
Аппаратные	Fortinet • Cisco • Juniper • Check Point (англ.)
FreeBSD	Ipfw • IPFilter • PF
Mac OS	NetBarrier X4 (англ.)
Linux	Netfilter (Iptables • Firestarter • Iplist • NuFW • Shorewall)

Прокси-серверы (proxy-servers) – это специальные серверы-посредники, через которые происходят обращения из локальной сети в глобальную. При этом обращения из глобальной сети в локальную становятся невозможными в принципе. Этот метод не дает достаточной защиты против атак на более высоких уровнях, например, на уровне приложения (вирусы, код Java и JavaScript).

VPN (виртуальная частная сеть) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). В зависимости от применяемых протоколов и назначения VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть. Используемые технологии: PPTP, PPPoE, IPSec. Виртуальные частные сети обеспечивают автоматическую защиту целостности и конфиденциальности сообщений, передаваемых через различные сети общего пользования, прежде всего, через Интернет. Фактически, VPN – это совокупность сетей, на внешнем периметре которых установлены VPN-агенты (рис. 1).

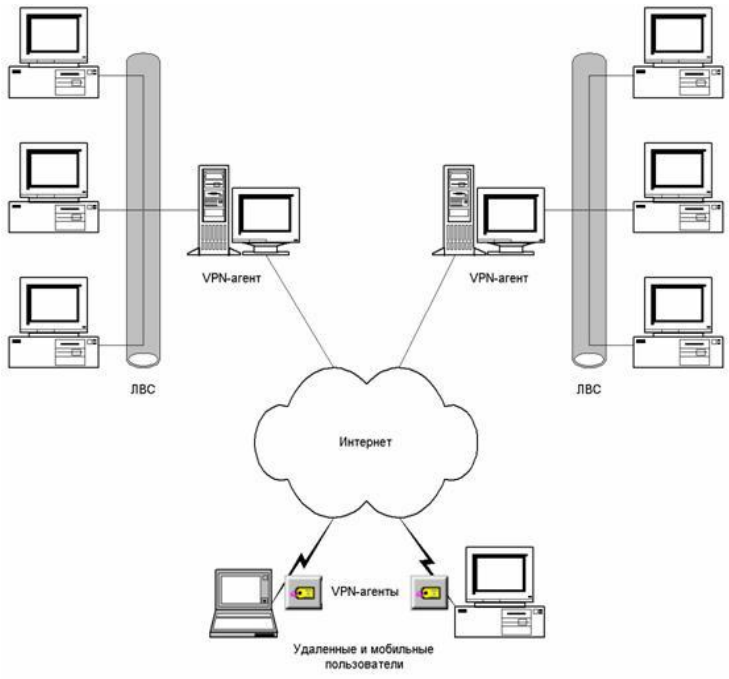

Рис. 1. Пример виртуальной частной сети

VPN-агент – это программа (или программно-аппаратный комплекс), обеспечивающая защиту передаваемой информации путем выполнения описанных ниже операций.

Перед отправкой в сеть любого IP-пакета VPN-агент производит следующее [3]:

1. Из заголовка IP-пакета выделяется информация о его адресате. Согласно этой информации на основе политики безопасности данного VPN-агента выбираются алгоритмы защиты (если VPN-агент поддерживает несколько алгоритмов) и криптографические

ключи, с помощью которых будет защищен данный пакет. В том случае, если политикой безопасности VPN-агента не предусмотрена отправка IP-пакета данному адресату или IP-пакета с данными характеристиками, отправка IP-пакета блокируется.

2. С помощью выбранного алгоритма защиты целостности формируется и добавляется в IP-пакет электронная цифровая подпись (ЭЦП), имитоприставка или аналогичная контрольная сумма.

3. С помощью выбранного алгоритма шифрования производится зашифрование IP-пакета.

4. С помощью установленного алгоритма инкапсуляции пакетов зашифрованный IP-пакет помещается в готовый для передачи IP-пакет, заголовок которого вместо исходной информации об адресате и отправителе содержит соответственно информацию о VPN-агенте адресата и VPN-агенте отправителя. То есть выполняется трансляция сетевых адресов.

5. Пакет отправляется VPN-агенту адресата. При необходимости производятся его разбиение и поочередная отправка результирующих пакетов.

При приеме IP-пакета VPN-агент производит следующее [3]:

1. Из заголовка IP-пакета выделяется информация о его отправителе. В том случае, если отправитель не входит в число разрешенных (согласно политике безопасности) или неизвестен (например, при приеме пакета с намеренно или случайно поврежденным заголовком), пакет не обрабатывается и отбрасывается.

2. Согласно политике безопасности выбираются алгоритмы защиты данного пакета и ключи, с помощью которых будут выполнены расшифрование пакета и проверка его целостности.

3. Выделяется информационная (инкапсулированная) часть пакета и производится ее расшифрование.

4. Производится контроль целостности пакета на основе выбранного алгоритма. В случае обнаружения нарушения целостности пакет отбрасывается.

5. Пакет отправляется адресату (по внутренней сети) согласно информации, находящейся в его оригинальном заголовке.

VPN-агент может находиться непосредственно на защищаемом компьютере (например, компьютеры «удаленных пользователей»). В этом случае с его помощью защищается информационный обмен только того компьютера, на котором он установлен, однако описанные выше принципы его действия остаются неизменными [3].

Основное правило построения VPN – связь между защищенной ЛВС и открытой сетью должна осуществляться только через VPN-агенты. Категорически не должно быть каких-либо способов связи, минующих защитный барьер в виде VPN-агента. То есть должен быть определен защищаемый периметр, связь с которым может осуществляться только через соответствующее средство защиты.

5. Специальные средства защиты от несанкционированного доступа

Для решения проблемы защиты компьютеров от НСД в большинстве операционных систем и популярных пакетов программ предусмотрены различные подсистемы защиты от НСД. Примером такой защиты является выполнение аутентификации пользователей при входе в операционные системы семейства Windows. Однако для серьезной защиты от НСД встроенных средств операционных систем недостаточно, так как периодически обнаруживаются уязвимости, которые позволяют получить доступ к защищаемым объектам в обход правил разграничения доступа. В связи с этим в дополнение к стандартным средствам защиты необходимо использование специальных средств ограничения или разграничения доступа [3].

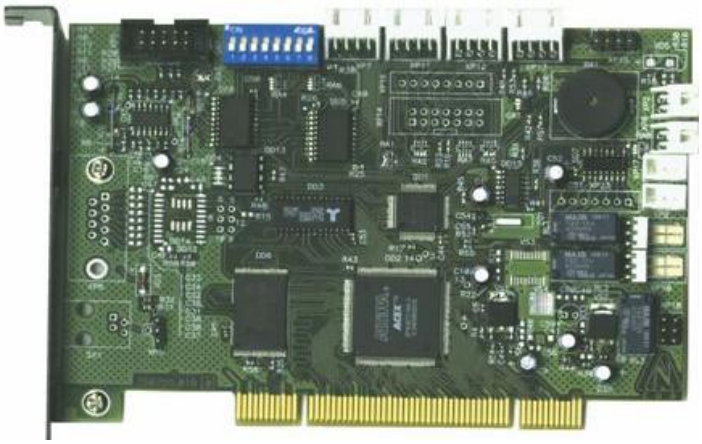

Рис. 2. Пример электронного замка

Наиболее надежное решение проблемы ограничения физического доступа к компьютеру – использование аппаратных средств защиты информации от НСД, выполняющихся до загрузки операционной системы. Такие средства защиты называются «электронными замками». Пример электронного замка представлен на рис. 2 [3].

Любое программное средство защиты может подвергнуться воздействию злоумышленника с целью искажения работы такого средства и последующего получения доступа к системе. В аппаратных средствах защиты все действия по контролю доступа пользователей электронный замок выполняет в собственной доверенной программе, которая не подвержена воздействиям извне.

На подготовительном этапе использования электронного замка выполняются его установка и настройка, включающая в себя следующие действия, обычно выполняемые ответственным лицом – Администратором по безопасности [3]:

1. Составление списка пользователей, которым разрешен доступ на защищаемый компьютер. Для каждого пользователя формируется ключевой носитель (в зависимости от поддерживаемых конкретным замком интерфейсов – дискета, электронная таблетка iButton или смарт-карта), по которому будет производиться аутентификация пользователя при входе. Список пользователей сохраняется в энергонезависимой памяти замка.

2. Составление списка файлов, целостность которых контролируется замком перед загрузкой операционной системы компьютера. Контролю также подлежат важные файлы операционной системы, например, системные библиотеки Windows, исполняемые модули используемых приложений, шаблоны документов Microsoft Word и т.д.

Контроль целостности файлов представляет собой вычисление их эталонной контрольной суммы, например, хэширование по алгоритму ГОСТ Р 34.11-94, сохранение вычисленных значений в энергонезависимой памяти замка, последующее вычисление реальных контрольных сумм файлов и сравнение с эталонными [3]. В штатном режиме работы электронный замок получает управление от BIOS защищаемого компьютера после включения последнего. На этом этапе и выполняются все действия по контролю доступа на компьютер, а именно [3]:

1. Замок запрашивает у пользователя носитель с ключевой информацией, необходимой для его аутентификации. Если ключевая информация требуемого формата не предъявляется или если идентифицируемый пользователь не входит в список пользователей защищаемого компьютера, замок блокирует загрузку компьютера.

2. Если аутентификация пользователя прошла успешно, замок рассчитывает контрольные суммы файлов, содержащихся в списке контролируемых, и сравнивает полученные контрольные суммы с эталонными. В случае, если нарушена целостность хотя бы одного файла из списка, загрузка компьютера блокируется. Для возможности дальнейшей работы на данном компьютере необходимо, чтобы проблема была разрешена Администратором, который должен выяснить причину изменения контролируемого файла и, в зависимости от ситуации, предпринять одно из следующих действий, позволяющих дальнейшую работу с защищаемым компьютером [3]:

– пересчитать эталонную контрольную сумму для данного файла, то есть зафиксировать измененный файл;

– восстановить исходный файл;

– удалить файл из списка контролируемых.

3. Если все проверки пройдены успешно, замок возвращает управление компьютеру для загрузки штатной операционной системы.

Так как описанные выше действия выполняются до загрузки операционной системы компьютера, замок обычно загружает собственную операционную систему (находящуюся в его энергонезависимой памяти. Обычно это MS-DOS или аналогичная ОС), в которой выполняются аутентификация пользователей и проверка целостности файлов. С точки зрения безопасности собственная операционная система замка не подвержена каким-либо внешним воздействиям, что не дает возможности злоумышленнику повлиять на описанные выше контролирующие процессы [3].

Информация о входах пользователей на компьютер, а также о попытках несанкционированного доступа сохраняется в журнале, который располагается в энергонезависимой памяти замка. Журнал может быть просмотрен администратором. При использовании электронных замков существует ряд проблем, в частности [3]:

1. BIOS некоторых современных компьютеров может быть настроен таким образом, что управление при загрузке не передается BIOS у замка. Для противодействия подобным настройкам замок должен иметь возможность блокировать загрузку компьютера в случае, если в течение определенного интервала времени после включения питания замок не получил управление.

2. Злоумышленник может просто вытащить замок из компьютера. Однако существует ряд мер противодействия: пломбирование корпуса компьютера, обеспечение отсутствия физического доступа пользователей к системному блоку компьютера, блокирование изнутри корпуса системного блока компьютера специальным фиксатором и т.д. Довольно часто электронные замки конструктивно совмещаются с аппаратным шифратором. В этом случае рекомендуемой мерой защиты является использование замка совместно с программным средством прозрачного (автоматического) шифрования логических дисков компьютера [3]. При этом ключи шифрования могут быть производными от ключей, с помощью которых выполняется аутентификация пользователей в электронном замке, или отдельными ключами, но хранящимися на том же носителе, что и ключи пользователя для входа на компьютер. Такое комплексное средство защиты не потребует от пользователя выполнения каких-либо дополнительных действий, но и не позволит злоумышленнику получить доступ к информации даже при вынутой аппаратуре электронного замка.

Если электронный замок разработан на базе аппаратного шифратора, получается одно устройство, выполняющее функции шифрования, генерации случайных чисел и защиты от НСД. Такой шифратор способен быть центром безопасности всего компьютера, на его базе можно построить полнофункциональную систему криптографической защиты данных, обеспечивающую, например, следующие возможности [3]:

- Защита компьютера от физического доступа.
- Защита компьютера от НСД по сети и организация VPN.
- Шифрование файлов по требованию.
- Автоматическое шифрование логических дисков компьютера.
- Вычисление/проверка ЭЦП.
- Защита сообщений электронной почты.

6. Выводы

Имея широкий спектр методов контроля соблюдения конфиденциальности компьютерных систем, специалисты должны сами подбирать оптимальный набор аппаратных и/или программных средств защиты под специфику и назначение систем, а также с учетом предъявленных к компьютерным системам требований заказчика.

В эпоху расцвета тотального международного шпионажа между развитыми странами проблема обеспечения и контроля конфиденциальности в области информационных технологий приобретает очень важное значение, особенно для открытых систем, имеющих выход в Интернет. Контроль соблюдения конфиденциальности КС может обеспечиваться программными, программно-аппаратными, организационными, смешанными и специальными средствами защиты, отдельные примеры которых приведены в данной работе. Имея широкий спектр различных средств контроля, специалисты могут сами подбирать оптимальный набор аппаратных и/или программных средств защиты с учетом специфики эксплуатации и назначения КС, а также с учетом предъявляемых к ним требований. Особое внимание данному вопросу необходимо уделять для КС критического применения, где несанкционированное проникновение в информационные и управляющие сегменты КС может повлечь за собой большие материальные, экологические и человеческие потери.

СПИСОК ЛИТЕРАТУРЫ

1. http://dic.academic.ru/dic.nsf/ruwiki/200171.
2. http://www.securitylab.ru/software/1308/page1_3.php.
3. http://www.panasenko.ru/Articles/77/77.html.

Стаття надійшла до редакції 22.05.2015