CNews.ru: Обзоры и обозрения
http://www.cnews.ru/reviews/free/security2007/articles/mobility.shtml

МОБИЛЬНОСТЬ ОБНАРУЖИВАЕТ НЕДОСТАТКИ

ЗА ТРИ КВАРТАЛА 2006 Г. ОБЪЕМЫ ПРОДАЖ НОУТБУКОВ В РОССИИ УВЕЛИЧИЛИСЬ НА 50% И ДОСТИГЛИ ОТМЕТКИ В 1 МЛН ШТ. ВСЁ БОЛЬШЕ РОССИЙСКИХ ПОЛЬЗОВАТЕЛЕЙ ДОВЕРЯЮТ ЭТИМ УСТРОЙСТВАМ ВАЖНУЮ ИНФОРМАЦИЮ, А ЗНАЧИТ, ТЕМ СЕРЬЕЗНЕЕ ЕЁ НЕОБХОДИМО ЗАЩИЩАТЬ. МОБИЛЬНОСТЬ УЖЕ НАЧИНАЕТ ОБНАРУЖИВАТЬ СВОЮ "ОБРАТНУЮ" СТОРОНУ.

К сожалению, такое качество как мобильность, преимущества которой для современного бизнеса сложно переоценить, на практике является еще и недостатком. Электрички, автобусы, салоны автомобилей, столики кафе становятся основными «зонами риска». Без сомнения, потерять мобильный телефон гораздо проще, чем переносной компьютер, но и ущерб от утраты этих двух устройств будет существенно различаться.

По данным CNews не менее 40% случаев утраты ноутбуков происходит вследствие их кражи. Какой ущерб наносится владельцу? Стоимость самого ноутбука за последние несколько лет существенно снизилась, в настоящее время редко превышая 30.000 – 35.000 руб. Плата за лицензию на операционную систему, как правило, включается в стоимость самого устройства. Суммарная стоимость программного обеспечения (ПО), установленного на ноутбуке, обычно составляет около 5-10 тыс. руб. К тому же, при сохранившихся дистрибутивах и регистрационных кодах не представляет труда установить всё ранее приобретённое ПО на другой компьютер. Таким образом, казалось бы, можно говорить об ущербе, не превышающем 45.000 руб. По Уголовному Кодексу такое хищение даже не попадает под определение «в крупном размере», не говоря уже об «особо крупном» (прим.4 к ст.158 Уголовного Кодекса РФ: «Крупным размером … признается стоимость имущества, превышающая двести пятьдесят тысяч рублей, а особо крупным - один миллион рублей»).

До 93% всех украденных ноутбуков уже никогда не возвращаются к владельцу. Ещё реже удаётся найти и привлечь к ответственности вора. Пойманному же преступнику грозит наказание «штрафом … либо обязательными работами на срок до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо арестом на срок от двух до четырех месяцев, либо лишением свободы на срок до двух лет».

Но, к сожалению, даже если преступник будет пойман и ноутбук вернётся к законному владельцу, то, скорее всего, все данные, хранившиеся на нем, будут уже уничтожены (форматирование жёсткого диска – одна из стандартных процедур «предпродажной» подготовки украденного ноутбука). Или же, по крайней мере, просмотрены и скопированы. Как успел распорядиться ими злоумышленник, и к каким последствиям приведут его действия - остаётся только догадываться.

Случаи целенаправленной «охоты» за лэптопами топ-менеджмента – частая практика на Западе. Ситуация в России пока относительно спокойна, но надолго ли?

Трудно спорить, что основной ущерб представляет утрата не самого ноутбука, а той информации, которая на нём хранилась. Если владелец не позаботился о дублировании диссертации, годового отчёта или материалов по стратегическому развитию компании – ущерб будет трудноооценим. Важную информацию никогда нельзя хранить в единственном экземпляре. Причём данная рекомендация относится не только к ноутбукам. Любой носитель данных может быть повреждён или утрачен. Резервное копирование решает эти и другие проблемы, причем совсем не обязательно использовать специализированные утилиты - достаточно просто скопировать нужные файлы штатными средствами.

К сожалению, утрата информации или только носителя (при наличии резервной копии) не худший вариант развития событий. Финансового директора крупной организации или руководителя службы безопасности банка, потерявшего ноутбук с конфиденциальной информацией, меньше всего интересует стоимость лицензий или самого устройства. А вот разглашение конфиденциальной информации о деятельности компании или её клиентах грозит не только судебными исками, но и другими, гораздо более серьёзным последствиями.

Для не самой крупной компании с годовым оборотом 5-10 млн руб. минимально возможный ущерб от попадания базы её клиентов в руки конкурента оценивается специалистами в 10% - 15% от оборота, что в 10 раз выше стоимости самого ноутбука. Возможны и более негативные события, вплоть до банкротства организации и ухода с рынка.

Не стоит также забывать, что если интерес представляет информация, хранящаяся на ноутбуке, то совсем не обязательно его похищать – достаточно получить к нему физический доступ на некоторое время.

МОБИЛЬНАЯ ЗАЩИТА

В наше время существует множество способов ограничить доступ злоумышленника к информации, хранящейся на ноутбуке или другом мобильном носителе. Самый очевидный – не дать его украсть. Не стоит оставлять его без присмотра в людных местах или в салоне автомобиля, особенно на видном месте, даже на пять минут, сумка ноутбука не должна привлекать внимание и позволять потенциальным злоумышленникам узнать о содержимом с первого взгляда.

Впечатляющая статистика по кражам красноречиво свидетельствуют о малой эффективности этих простых правил в повседневной жизни. Это дало толчок появлению самых разных решений, направленных на предотвращение кражи мобильных устройств. Так, компания SlappingTurtle предлагает установить на лэптоп сигнализацию, аналогичную автомобильной. В «антиугонном» режиме, при любом перемещении компьютера, раздаётся резкий звук, призванный предупредить владельца о возможной опасности. Однако ноутбук все это время должен находиться во включенном состоянии. Если каким-то образом компьютер удастся отключить или, допустим, у него сядет батарея - такой метод защиты потеряет всякий смысл.

Другой подход предлагает компания Everdream. Программная защита, установленная на ноутбук, позволяет удалённо подать команду на шифрование конфиденциальных данных, а также определить местоположение ноутбука. Данный процесс запускается автоматически после звонка пользователя. Но при этом злоумышленник должен выйти в интернет с данного лэптопа. Будет ли злоумышленник подключаться к глобальной сети с украденного ноутбука? Ведь цель преступника – содержимое самого компьютера, а им он может воспользоваться и так.

Есть и простейший способ защиты, с успехом применяемый велолюбителями. Специальным устройством-замком ноутбук прочным тросом можно «пристегнуть» к какому-либо предмету, который нельзя унести (батарея, столб и т.п.).

Трос может оказаться прочным, но сказать то же самое оместе его крепления к ноутбуку – вряд ли возможно. К тому же, для «охотниказа информацией» основной интерес представляет жёсткий диск компьютера, а неего корпус. С другой стороны, много ли столбов или батарей, допустим, вконференц-зале или аэропорту?

Наиболее распространенными и простыми в эксплуатацииспособами защиты по-прежнему являются встроенные возможности - такие какпароль BIOS, парольучётной записи при входе в операционную систему и блокировка при бездействиипользователя. Данные методы могут служить лишь дополнительной меройбезопасности. Квалифицированного злоумышленника такие барьеры, конечно, не остановят.

Главным же способом предотвращения несанкционированного доступа к информации было и остаётся применение шифрования данных. Долгое время на рынке присутствовали только программные решения, сейчас уже и производители аппаратных устройств начинают встраивать алгоритмы шифрования в свои продукты. Рассмотрим подробнее некоторые из них.

АППАРАТНОЕ ШИФРОВАНИЕ

Hardware-Based Full Disc Encryption. Ещё в 2005 году компания Seagate Technology представила технологию аппаратного шифрования информации Hardware-Based Full Disc Encryption (FDE).

В конце 2006 года она получила развитие – был анонсирован жёсткий диск Seagate Momentus 5400 FDE.2 Если верить сайту price.ru, то модель 160Gb в мае можно было даже купить за 4.333 руб.

Для сравнения, аналогичная модель без поддержки FDE.2 была заявлена на том же сайте по цене 3.478 руб. Что же получает пользователь за 855 руб.?

Технология FDE позволяет автоматически шифровать все данные, записываемые на диск, включая информацию для разметки диска, системные файлы и данные самого пользователя.

В FDE.2 используется алгоритм AES с длиной мастер-ключа 128 бит (ранее применялся TripleDES). Программный код реализации алгоритма хранится и исполняется в микрокоде прошивки контролера диска.

Доступ к диску возможен только после ввода пользователем пароля. Детального описания технологии на сайте производителя не представлено, но так как пароль пользователя явно может быть сменён по его (пользователя) желанию, очевидно, что сами ключи шифрования не генерируются из пароля. Ведь иначе при смене пароля пришлось бы перешифровывать все данные на новом мастер-ключе, а для диска в 160 Гб эта процедура довольно продолжительна.

Общеизвестен принцип «слабого звена»: безопасность системы определяется безопасностью её самого слабого элемента. Таким образом, вся защита фактически построена на незнании злоумышленником пароля. После этого не так уж и важно, каким алгоритмом зашифрованы сами данные. К вопросу парольной защиты мы ещё вернёмся.

В одном из рекламных проспектов как о преимуществе говорится о том, что «вычислительная платформа жесткого диска не является открытой, как платформа ПК, а сам винчестер обладает уникальной, свойственной только ему, архитектурой, данные о которой берегутся производителями». Однако, любой специалист по информационной безопасности и криптографии понимает, что нельзя всерьёз полагаться на незнание злоумышленником принципа работы системы, т.к. с помощью современных технологий реинжиниринга и дизассемблирования можно по шагам проследить все действия программы и понять её алгоритм работы. Безусловно, для работы с содержимым микросхемы жёсткого диска потребуется специальное оборудование, но его стоимость и стоимость таких работ может оказаться незначительной по сравнению с потенциальной стоимостью конфиденциальной информации.

К тому же не стоить сбрасывать со счетов промышленный шпионаж, злонамеренные действия инсайдера и другие каналы утечки данных из отдела разработок. Для сохранения в тайне какого-либо алгоритма, над которым трудятся десятки людей потребуются затраты, значительно повышающие себестоимость устройства.

Приобретение данного жёсткого диска для замены своего основного представляется нецелесообразным, т.к. к сожалению, для работы с диском требуется поддержка его в BIOS – первоначальный запрос пароля пользователя нужно вывести на монитор, а сам пароль считать с клавиатуры. Сделать это самостоятельно микроконтроллер диска не в состоянии. Поэтому просто купить Momentus и установить его в свой компьютер не получится. В марте этого года компания ASI Computer Technologies объявила о своих планах по выпуску моделей ноутбуков, оснащённых жёсткими дисками Segate Momentus 5400 FDE.2 Стоимость в базовой конфигурации заявлена в 2.150 долларов.

По словам представителей компании, Seagate ведет переговоры с другими производителями ноутбуков о включении в конфигурацию моделей дисков с технологией шифрования (по сообщению Fox News).

Trusted Platform Module. Производителем Momentus 5400 FDE.2 заявлена поддержка модуля "доверенных платформ" (Trusted Platform Module, TPM). TPM - это аппаратное устройство, подключенное к системной плате платформы и предназначенное для подтверждения идентичности и проверки рабочих параметров компьютера.

Если описать упрощённо, то TPM хранит значение хэш-функции (например, SHA1 – Secure Hash Algorithm) от основных параметров ключевых компонентов системы: видеокарты, процессора, файлов операционной системы и т.п.

При загрузке компьютера данное значение вычисляется и сверяется с эталонным. Компьютер будет стартовать в «проверенном состоянии» (authorized condition) только в том случае, если TPM получит правильное значение хэша. В проверенном состоянии операционная система получает доступ к корневому ключу шифрования (encrypted root key), который требуется для работы приложений и доступа к данным, защищённым системой TPM. Если при загрузке было получено неправильное значение хэша, то система считается не доверяемой, и в ней будут доступны только обычные, не конфиденциальные файлы и программы.

TPM и хранящиеся в нем данные изолированы от остальных компонентов платформы. Модуль TPM защищает пользовательские данные и аппаратно реализует алгоритмы шифрования и электронной цифровой подписи.

Хранить ключи шифрования в таком устройстве гораздо безопаснее, чем в самом микроконтроллере жёсткого диска, какой бы закрытой и малоизученной ни была его архитектура.

К сожалению, в Россию поставки ноутбуков происходят исключительно с деактивированным модулем TPM. Связано это с экспортно-импортными ограничениями на криптографические устройства.

Encrypted Hard Drive Enclosure. Компания COOLGear предлагает внешние контейнеры стоимостью 129,98 долларов для 3,5 и 2,5 дюймовых дисков с аппаратной поддержкой алгоритмов шифрования DES и TripleDES. По запросу возможна поставка с алгоритмом шифрования с длиной ключа 192 бита.

Устройства комплектуются аппаратным ключом, подключаемым к специальному разъёму 6-pin 1394a. Именно на этом устройстве и хранятся ключи шифрования. Процедуры смены ключа шифрования и перешифрования диска не предусмотрены.

Внутреннее устройство аппаратного ключа на сайте производителя не раскрывается. Не исключено, что в основе лежит обычная flash-память, доступ к которой возможен в обход штатных методов – прямым чтением после вскрытия корпуса устройства.

Понятно, что системный раздел жёсткого диска ноутбука с помощью этого устройства зашифровать не получится. Соответственно, на жёстком диске, помещённом в данный контейнер, будут храниться преимущественно данные. Но для шифрования в настоящее время доступно огромное количество программ и утилит на любой вкус и за гораздо меньшие деньги. Высокая производительность (главный аргумент сторонников аппаратного шифрования) при работе с данными не требуется (в отличие от случая, когда зашифрованы исполняемые файлы), поэтому целесообразность использования таких устройств не очевидна.

ЭКСПОРТНО-ИМПОРТНЫЕ ОГРАНИЧЕНИЯ

Чтобы официально ввезти устройство с аппаратно реализованным «стойкими» криптографическим алгоритмом или диск с программным обеспечением, реализующим такие алгоритмы, нужно соответствующее разрешения Минэкономразвития (для получения которого в свою очередь необходима

лицензия ФСБ). Получить это всё не так просто, особенно если речь идёт о действительно надёжных средствах шифрования.

Из-за этого часто аппаратные шифросредства поставляются в так называемом «деактивированном» виде, а в программных продуктов оставляется только поддержка «слабых» криптографических алгоритмов. Нередко такие поставки сопровождаются комментарием производителя о невозможности активации заблокированных функций, но на тематических форумах в сети не так сложно найти инструкции по снятию блокировки чуть ли не штатными средствами с компакт-диска, идущего в комплекте. Из-за этого лицензирующие органы не очень «любят» такие продукты.

Один из основных камней преткновения - Указ Президента РФ от 3 апреля 1995 г. N 334 "О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации".

Многие специалисты в области юриспруденции и права полагают, что данный документ фактически прекратил своё действие или даже вообще никогда не имел юридической силы, т.к. президент по российскому законодательству не имеет права изменять федеральные законы, а именно федеральный закон определяет перечень лицензируемых видов деятельности.

Несмотря на всё это на практике данный указ применяется, в том числе и в части, касающейся ограничения ввоза: «*Государственному таможенному комитету Российской Федерации принять меры к недопущению ввоза на территорию Российской Федерации шифровальных средств иностранного производства без лицензии Министерства внешних экономических связей Российской Федерации, выданной по согласованию с Федеральным агентством правительственной связи и информации при Президенте Российской Федерации*».

По одной из версий, возникшей в первые дни после прошлогодних громких обысков в офисах компаний, те события были связаны как раз с нарушением данного указа, а именно – с «незаконными» поставками ноутбуков с TPM. Впоследствии, как известно, эта версия не подтвердилась, но, тем не менее, пока легально использовать TPM на территории нашей страны проблематично. Возможно, что ситуация изменится после вступления России в ВТО.

«Серые» и полулегальные поставки, а также самостоятельную (нештатную) активацию заблокированных функций вряд ли вообще имеет смысл рассматривать, если вы хотите защищать действительно конфиденциальную информацию. Это равносильно использованию для защиты информации и шифрования данных «взломанных» программ, не требующих наличия лицензии. Бреши в системе безопасности, возникшие после использования таких программных или аппаратных средств, могут оказаться серьёзней, чем в случае полного их (средств) отсутствия.

ПРОГРАММНОЕ ШИФРОВАНИЕ

Программные средства для шифрования данных появились достаточно давно. Так, например, Secret Disk продаётся с конца 90-х годов. На протяжении всего этого длительного промежутка времени данные решения постоянно развивались и совершенствовались. На сегодняшний день на рынке присутствуют профессиональные решения, которые можно использовать как для защиты личной информации в повседневной жизни, так и для надёжного шифрования корпоративных данных.

Как правило, в программных продуктах выбор алгоритмов шифрования по сравнению с аппаратными решениями достаточно широк (минимум 3-4 алгоритма с различными длинами ключей) и может легко увеличиваться за счёт внешних подключаемых модулей.

В современных продуктах проблема снижения производительности из-за использования шифрования уже не является актуальной. Во всех продуктах - лидерах рынка реализована поддержка многопоточного

шифрования и многопроцессорных (многоядерных) систем. Современные решения позволяют шифровать в том числе и системный раздел без каких-либо существенных потерь производительности.

По мнению специалистов, на сегодняшний день любой современной криптографической системе вполне достаточно 128-битового уровня безопасности. Это означает, что для осуществления успешной атаки на такую систему потребуется, как минимум, 2128 шагов. Согласно закону Мура, адаптированного к криптографии, достаточно даже 110 или 100 бит, однако криптографических алгоритмов, рассчитанных на такие ключи, не существует.

Сам алгоритм должен быть максимально широко распространён. Никому неизвестные «самописные» алгоритмы не изучены специалистами в области криптографии и могут содержать опасные уязвимости. Таким образом, достаточно надёжными могут быть признаны алгоритмы ГОСТ, AES, Twofish, Serpent с длиной ключа 128, 192 или 256 бит.

Отдельного рассмотрения заслуживают асимметричные алгоритмы шифрования. В них для шифрования и расшифрования используются разные ключи (отсюда и их название). Эти ключи образуют пару и генерируются, как правило, самим пользователем. Для шифрования информации используется т.н. открытый ключ. Этот ключ общеизвестен и любой желающий может зашифровать адресуемое пользователю сообщение с его помощью. Закрытый ключ используется для расшифрования сообщения и известен только самому пользователю, который хранит его в секрете.

Общепринятым способом распространения и хранения открытых ключей пользователей является использование цифровых сертификатов формата X.509 Цифровой сертификат в простейшем случае – это своего рода электронный паспорт, который содержит информацию о пользователе (имя, идентификатор, адрес электронной почты и т.п.), информацию об открытом ключе клиента, об Удостоверяющем центре, изготовившем сертификат, серийный номер сертификата, срок действия и т.д.

Удостоверяющий Центр (УЦ) — это третья доверительная сторона, которая наделена высоким уровнем доверия пользователей и которая обеспечивает комплекс мероприятий для использования доверяющими сторонами сертификатов. Удостоверяющий центр — это компонент системы управления сертификатами, предназначенный для формирования электронных сертификатов подчиненных центров и конечных пользователей, удостоверенных электронно-цифровой подписью УЦ.

В простейшем случае используются т.н. самоподписанные сертификаты, когда пользователь сам выступает в роли своего удостоверяющего центра.

Общепризнано, что в случае использования асимметричных алгоритмов шифрования, эквивалентная 128-битному симметричному алгоритму стойкость достигается при использовании ключей длиной не менее 1024 бит. Это связано с особенностями математической реализации таких алгоритмов.

Асимметричные алгоритмы не применяются для шифрования данных, так как из-за сложных математических преобразований, они работают крайне медленно. С помощью этих алгоритмов обычно шифруется ключ (например, 128 бит), с помощью которого каким-либо симметричным алгоритмом шифруются уже сами данные.

ЗАКРЫТЫЙ КЛЮЧ – ВСЕМУ ГОЛОВА

Современные алгоритмы шифрования достаточно надёжны. Использование ключей шифрования длиной 128 бит надёжно защитит информацию как минимум на ближайшие 10-15 лет. Поэтому основной проблемой является безопасное хранение ключей шифрования. Человек, к сожалению, не в состоянии запомнить случайные 128 бит информации, а значит, их нужно где-то сохранить. Понятно, что хранить ключи шифрования в открытом виде недальновидно,т.к. слишком ненадёжно.

В наиболее простых продуктах ключи шифрования защищаются (зашифровываются) паролем, который вводит сам пользователь. Подобный подход серьёзно снижает общий уровень безопасности системы. Например, для полного перебора крайне сложного для запоминания 8-ми символьного пароля из случайной последовательности символов латинского алфавита (заглавные и строчные буквы), цифр (0, 1, … 9) и некоторых знаков («плюс», «минус») потребуется проверить (26+26+10+2)8 = 648 = 240 вариантов. Таким образом, фактически длина ключа снижается со 128 до 40 (!) бит. Какого-либо смысла использовать в таких случаях надёжные алгоритмы шифрования данных – попросту нет, т.к. злоумышленнику гораздо проще осуществить атаку на пароль пользователя, чем пытаться подобрать 128-битный ключ шифрования. Как показывает практика, пользователи зачастую выбирают ещё более простые пароли, подверженные словарным атакам. Для подбора таких паролей потребуется ещё меньше времени.

Для повышения безопасности производители предлагают использовать специальные ключевые контейнеры для хранения ключей шифрования. Такие контейнеры размещаются обычно в каком либо файле (например, *.mp3 или *.jpg). Но, к сожалению, данный способ не сильно усложняет взлом системы – любые такие файлы имеют чёткую структуру, определяемую их форматом и выявить «неправильный» файл, даже если он один из ста в каталоге, особого труда не составит.

В некоторых продуктах ключи шифрования, защищённые паролем, можно сохранять на внешних носителях. Крайне не рекомендуется в качестве внешнего носителя использовать дискету, CD или USB-flash. Доступ к содержимому этих носителей никак не ограничивается, а для изготовления дубликата достаточно нескольких минут.

Гораздо надёжнее хранить ключи шифрования (защищённые паролем) на специальных устройствах - токенах, которые могут выступать в виде смарт-карты или USB-устройства. Доступ к их памяти возможен только после ввода правильного PIN-кода. Сам PIN-код предполагает набор из различных символов, букв и цифр. Наиболее современные модели токенов имеют обязательное аппаратное ограничение на количество попыток неправильного вода PIN-кода. После превышения заданного лимита устройство блокируется и дальнейшие попытки подбора будут безрезультатны.

Однако есть ещё более надёжный способ защиты ключей шифрования. Дело в том, что современные токены позволяют не только хранить в закрытой памяти данные, но также выполняют аппаратно целый ряд криптографических преобразований. Так, например, смарт-карты, а также USB-ключи, являющиеся полнофункциональными смарт-картами, а не их аналогами, реализуют асимметричные алгоритмы шифрования. Примечательно, что при этом пара открытый – закрытый ключ генерируется также аппаратно. Важно, что закрытый ключ на смарт-картах хранится как «write-only», т.е. он используется операционной системой смарт-карты для криптографических преобразований, но не может быть прочитан или скопирован пользователем. Фактически, пользователь сам не знает свой закрытый ключ – он только им обладает.

Данные, которые необходимо расшифровать, передаются операционной системе смарт-карты, аппаратно ей расшифровываются с помощью закрытого ключа и передаются обратно в расшифрованном виде. Все операции с закрытым ключом возможны только после ввода пользователем PIN-кода от смарт-карты.

Такой подход успешно используется во многих современных информационных системах для аутентификации пользователя. Применим он и для аутентификации пользователя при доступе к зашифрованной информации. Мастер-ключ (ключ на котором зашифрованы сами данные), шифруется с помощью открытого ключа пользователя. Для получения доступа к данным пользователь предъявляет свою смарт-карту (или USB-ключ, являющийся полнофункциональной смарт-картой) и вводит PIN-код от неё. Затем мастер-ключ аппаратно расшифровывается с помощью закрытого ключа, хранящегося на смарт-карте, и пользователь получает доступ к данным. Такой подход сочетает в себе безопасность и удобство использования.

ШИФРОВАНИЕ МАСТЕР - КЛЮЧА С ИСПОЛЬЗОВАНИЕМ АСИММЕТРИЧНОГО АЛГОРИТМА ШИФРОВАНИЯ

Современные токены поддерживают асимметричные алгоритмы с длиной ключа 1024 или 2048 бит, обеспечивая тем самым соответствие надёжности алгоритма шифрования мастер-ключа и надёжности алгоритма шифрования самих данных (дело в том, что асимметричные алгоритмы в силу своих математических особенностей требует длин ключей 1024 бит для получения уровня безопасности, соответствующего симметричным 128-битные алгоритмам).

Аппаратное ограничение на количество неправильных попыток ввода PIN-кода нивелирует риск его подбора и позволяет использовать достаточно простой для запоминания PIN-код. Создать дубликат смарт-карты не может даже сам пользователь, т.к. нет возможности скопировать закрытый ключ.

Актуальность темы, открытость криптографических алгоритмов и большое количество готовых криптографических библиотек привело к тому, что на рынке представлено просто огромное количество самых разнообразных программных продуктов для шифрования данных. Большинство из них ограничивает доступ только с помощью паролей. Недостатки такого подхода были рассмотрены выше.

Любой современный профессиональный продукт этого класса помимо обязательной поддержки смарт-карт и токенов должен иметь функционал шифрования системного раздела жёсткого диска.

Это позволяет избежать уязвимости, связанные с особенностью работы операционной системы. Шифрование отдельных файлов или разделов жёсткого диска с помощью программного обеспечения не обеспечивает полной защиты информации, так как у злоумышленника остается возможность восстановить часть или даже целые файлы из временных каталогов, резервных копий и других «внутренних источников» операционной системы.

Есть два подхода к шифрованию системного раздела: полное шифрование жёсткого диска – Full Disk Encryption (FDE); а также шифрование системного раздела – System Disk Encryption (SDE).

В первом случае после успешной аутентификации и загрузки операционной системы пользователь получает полный доступ ко всему диску. Во втором же – данные на системном и несистемных дисках шифруются независимо. При этом доступ к системному диску может иметь, например, пользователь компьютера и администратор организации, а доступ к разделу с данными – только пользователь. Такой подход позволяет провести дополнительное разграничение прав доступа.

СРАВНЕНИЕ АППАРАТНОГО И ПРОГРАММНОГО ШИФРОВАНИЯ

Параметр	**Аппаратное шифрование**	**Программноешифрование**
Падение производительности	Минимально, однако, всё равноприсутствует. Что бы не заявляли производители, любое преобразование данныхтребует времени на	Зависит от качества самого программногопродукта. У лучших разработчиков редко превышает т 5%, что не существенно.

	обработку	
Поддерживаемые операционные системы	Любые.	Только поддерживаемые производителем.
Безопасность	Обеспечивается незнанием злоумышленником пароля. Как вариант - использование TPM.	Парольи/или внешние криптографические устройства (электронные USB-ключи и смарт-карты).
Поддерживаемые алгоритмы шифрования	Только встроенные разработчиком.	Любые,при возможности подключения внешних модулей.
Разграничение доступа	Full disk encryption. Шифруются все данные. Знаниепароля предоставляет доступ ко всем данным на жёстком диске.	System disk encryption. Администратор может загрузитькомпьютер и получить доступ к системному разделу, но не к самим данным.Пользователь имеет полный доступ.
Типы защищаемых носителей	Жёсткиедиски. Для шифрования системного раздела требуется совместимая версия BIOS.	Любые,включая CD, DVD и flash-память.
Стоимость	От 129,98долларов за мобильный контейнер.	От 4.720руб. за версию с электронным USB-ключом.

Мобильные технологии получают всё большее распространение, проникая в нашу повседневную жизнь и создавая комфортные условия для ведения бизнеса. Количество продаваемых ноутбуков постоянно увеличивается и вполне вероятно скоро сравняется с количеством продаваемых настольных компьютеров. Всё большее количество конфиденциальных данных хранящихся на компьютерах коммерческих организациях и государственных учреждений оказывается вне стен здания и подвергается риску.

Стоимость систем шифрования данных не идёт ни в какое сравнение со стоимостью информации, хранящейся порой на ноутбуках, а точнее – с возможным ущербом от её раскрытия. Крупные компании, дорожащие своей репутацией, это уже осознали, поэтому популярность таких систем постоянно растёт. Как люди сугубо прагматичные, корпоративные пользователи выбирают профессиональные системы, главный акцент при разработке которых производитель сделал именно на высоком уровне обеспечиваемой безопасности.

Появившиеся на рынке более десяти лет тому назад программные продукты на сегодняшний день представляют собой зрелые, проверенные временем решения, которым без опасения можно доверять самую ценную информацию.

Сравнительно недавно разработанные жёсткие диски и мобильные контейнеры со встроенными алгоритмами шифрования пока мало подходят для корпоративного использования, а так же имеют ряд технологических ограничений, но в определённых ситуациях при сугубо домашнем использовании могут стать неплохой альтернативой программным решениям.

Рынок аппаратных средств для шифрования жёстких дисков на нынешнем этапе своего развития производит впечатление только зарождающегося. Устройства единичны, а их сравнения, описываемые в СМИ, чаще всего носят скорее маркетинговый нежели технологический характер. Тот факт, что такой крупный производитель, как Seagate, разрабатывает данное направление, позволяет надеяться на появление в будущем действительно надёжных и функциональных устройств, пока же реальную конкуренцию программным средствам аппаратные решения вряд ли могут составить.

С учётом особенностей российского законодательства, использование как аппаратных, так и программных средств иностранного производства имеет ряд нюансов. В качестве рекомендации можно посоветовать использовать сертифицированные продукты или продукты российского производства.