# КАК ВЫБРАТЬ СИСТЕМУ ШИФРОВАНИЯ ДАННЫХ?

По меткому выражению аналитиков CNews: 2005 год в России прошел под девизом «защищаемся от внутренних угроз». Тенденции прошлого года продолжили своё развитие и в нынешнем. Анализируя недавние инциденты, связанные с кражей баз данных и их последующей свободной продажей, многие компании стали более серьёзно задумываться о проблеме безопасности своих информационных ресурсов и разграничении прав доступа к конфиденциальным данным. Как известно, получить 100% гарантию сохранности ценной информации практически невозможно, но технологически свести такие риски к минимуму можно и нужно. Для этих целей большинство разработчиков средств информационной безопасности предлагают использовать комплексные решения, сочетающие шифрование данных с контролем сетевого доступа. Попробуем разобраться с такими системами более детально.

На сегменте рынка средств защиты от НСД представлено достаточно много разработчиков программно-аппаратных комплексов шифрования для серверов, хранящих и обрабатывающих конфиденциальную информацию (Aladdin, SecurIT, Физтехсофт и др.). Разобраться в тонкостях каждого предлагаемого решения и выбрать оптимальное подчас непросто. К сожалению, зачастую авторы сравнительных статей, посвященных шифро-средствам, не учитывая специфики этой категории продуктов, проводят сравнение удобства использования, богатства настроек, дружелюбности интерфейса и т.п. Такое сравнение оправдано, когда речь идёт о тестировании интернет-пейджеров или менеджеров закачек, но вряд ли приемлемо при выборе решения для защиты конфиденциальной информации.

Может быть мы сейчас не откроем Америку, но такие характеристики как производительность, стоимость и многие другие не являются критическими при выборе системы шифрования. Та же производительность важна не для всех и не всегда. Скажем, если в организации доступ к зашифрованной информации будут иметь только два сотрудника, а пропускная способность локальной сети небольшая, то пользователи вряд ли вообще заметят систему шифрования, даже самую «неторопливую».

Многие другие особенности и параметры таких программно-аппаратных комплексов также носят избирательный характер: для кого-то они критичны, а кому-то безразличны. Поэтому мы попробуем предложить альтернативный вариант сравнения по наиболее важным и действительно ключевым параметрам средств защиты от НСД и утечки конфиденциальной информации.

## ШТИРЛИЦ, ДЛЯ ВАС ШИФРОВКА!

При выборе системы для защиты данных, прежде всего, стоит обратить внимание на используемые **алгоритмы шифрования**.

Теоретически, приложив достаточно усилий, злоумышленник может взломать любую криптографическую систему. Вопрос заключается лишь в том, сколько работы ему необходимо для этого проделать. В принципе, фактически любую задачу по взлому криптографической системы количественно можно сравнить с поиском, выполняемым путём полного перебора всех возможных вариантов.

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.

Помимо непосредственно алгоритмов шифрования стоит обратить внимание и на способ их реализации. Программно-аппаратный комплекс может иметь встроенные алгоритмы шифрования или использовать внешние подключаемые модули. Второй вариант предпочтительнее по трём причинам. Во-первых, вы сможете повышать уровень безопасности, в соответствии с растущими потребностями компании, используя более стойкие алгоритмы Опять же, в случае изменения требований политки безопасности (например, компании потребуется переход на сертифицированные криптопровайдеры) вы сможете оперативно заменить имеющиеся криптоалгоритмы, на требуемые без какой-либо существенной задержки или сбоя в работе. Понятно, что в случае встроенной реализации алгоритма это гораздо сложнее.

Второй плюс внешней реализации заключается в том, что такое шифросредство не подпадает под соответствующие законодательные ограничения по его распространению, в т.ч. экспортно-импортные, не требует наличия у партнеров компании, занимающихся его распространением и внедрением, наличия соответствующих лицензий ФСБ.

И, в-третьих, не стоит забывать и о том, что реализация алгоритма шифрования – далеко не тривиальная задача. Правильная реализация требует большого опыта. Скажем, ключ шифрования никогда не должен находиться в оперативной памяти компьютера в явном виде. В серьёзных продуктах этот ключ разделяется на несколько частей, при этом на каждую из них накладывается случайная маска. Все операции с ключом шифрования производятся по частям, а на итоговый результат накладывается обратная маска. Уверенности в том, что разработчик учёл все эти тонкости при самостоятельной реализации алгоритма шифрования, к сожалению, нет.

## «А МОЖЕТ ТЕБЕ, МАЛЬЧИК, ЕЩЕ КЛЮЧ ОТ КВАРТИРЫ ДАТЬ, ГДЕ ДЕНЬГИ ЛЕЖАТ?»

Ещё одним фактором, влияющим на степень защищённости Ваших данных, является принцип организации **работы с ключами шифрования**. Здесь есть несколько вариантов, и перед выбором конкретной системы шифрования настоятельно рекомендуется поинтересоваться, как она устроена: где хранятся ключи шифрования, как они защищаются и т.д. К сожалению, зачастую сотрудники компании-разработчика не в состоянии объяснить даже базовых принципов работы их продукта. Особенно это замечание относится к т.н. sales-менеджерам. Простейшие вопросы нередко ставят их в тупик. Пользователю же, решившему защитить свою конфиденциальную информацию, желательно разобраться во всех тонкостях.

Для определённости будем называть ключ, используемый для шифрования данных мастер-ключом.

На сегодняшний день наиболее распространенными и часто используемыми являются следующие два подхода.

1. **Мастер-ключ генерируется на основе некоторых входных данных**. Этот мастер-ключ используется при шифровании данных. В дальнейшем для получения доступа к зашифрованной информации пользователь вновь предоставляет системе те же самые входные данные для генерации мастер-ключа. Сам мастер-ключ, таким образом, нигде не хранится.

   Основным недостатком этого способа является невозможность создания резервной копии мастер-ключа. В качестве входных данных могут быть использованы: пароль, какой-либо файл, сохранённый на внешнем носителе и т.п. Утрата любого компонента входных данных ведёт к утрате доступа к вашей информации.

2. **Мастер-ключ генерируется с использованием генератора случайных чисел**. Затем он шифруется каким-либо алгоритмом и после этого сохраняется вместе с данными или же на внешнем носителе. Для получения доступа сначала расшифровывается мастер-ключ, а после этого – сами данные. Для шифрования мастер-ключа целесообразно использовать алгоритм такой же стойкости, что и для шифрования самих данных. Использование менее стойкого алгоритма снижает безопасность системы, а использование более стойкого - бессмысленно, т.к. безопасность не повышает.

   В общем случае, надёжность криптографической системы определяется надёжностью самого слабого её звена. Злоумышленник всегда может атаковать наименее стойкий алгоритм из двух: алгоритм шифрования данных или алгоритм шифрования мастер-ключа.

   Второй подход позволяет создавать резервные копии мастер-ключа, которые возможно использовать в дальнейшем для восстановления доступа к данным в случае каких-либо форс-мажорных обстоятельств.

Ключ, на котором осуществляется шифрование мастер-ключа, также получают на основе некоторых входных данных. Рассмотрим этот вопрос более подробно.

### ВАРИАНТ ПЕРВЫЙ: ПАРОЛЬНЫЙ

Пользователь вводит некоторый пароль, на основе которого с использованием, например, хэш-функции генерируется ключ шифрования (см. схему №1). Фактически надёжность системы в этом случае определяется только сложностью и длиной пароля. Использование надёжных паролей неудобно: запомнить бессмысленный набор из 10-15 символов и вводить его каждый для получения доступа к данным не так просто. А если таких паролей несколько (допустим, для доступа к разным приложениям), то и вовсе невозможно. Парольная защита также подвержена атакам методом прямого перебора, а установленный клавиатурный шпион легко позволит злоумышленнику получить доступ к данным.

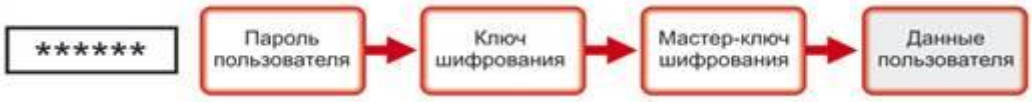


СХЕМА №1. ШИФРОВАНИЕ МАСТЕР-КЛЮЧА С ИСПОЛЬЗОВАНИЕМ ПАРОЛЯ

## ВАРИАНТ ВТОРОЙ: ВНЕШНЕЕ ХРАНЕНИЕ

На внешнем носителе размещаются некоторые данные, используемые для генерации ключа шифрования (см. схему №2). Простейшим вариантом является использование файла (т.н. ключевой файл), расположенного на дискете (CD-диске, USB-флэш памяти и т.п.) Этот способ надёжнее варианта с паролем. Для генерации используются не десяток символов пароля, а значительное количество данных, например, 64 или даже 128 байт.

В принципе, ключевой файл можно разместить и на жёстком диске компьютера, но значительно безопасней хранить его отдельно от данных.

Не рекомендуется в качестве ключевых файлов использовать файлы, создаваемые какими-либо общеизвестными приложениями (*.doc, *xls, *.pdf и т.д.) Их внутренняя структурированность может дать злоумышленнику дополнительную информацию. Например, все файлы, созданные архиватором WinRAR, начинаются с символов «Rar!» - это целых четыре байта.

Недостатком данного способа является возможность для злоумышленника легко скопировать файл и создать дубликат внешнего носителя. Таким образом, пользователь, даже на короткое время утративший контроль над этим носителем, фактически уже не может быть на 100% уверен в конфиденциальности своих данных.

В качестве внешнего носителя иногда применяются электронные USB-ключи или смарт-карты, но при этом данные, используемые для генерации ключа шифрования, просто сохраняются в памяти этих носителей и так же легко доступны для считывания.


СХЕМА №2. ШИФРОВАНИЕ МАСТЕР-КЛЮЧА С ИСПОЛЬЗОВАНИЕМ ДАННЫХ С ВНЕШНЕГО НОСИТЕЛЯ (ДИСКЕТА, CD-ДИСК).

## ВАРИАНТ ТРЕТИЙ: ЗАЩИЩЕННОЕ ВНЕШНЕЕ ХРАНЕНИЕ.

Данный способ во многом схож с предыдущим. Важным отличием является то, что для получения доступа к данным на внешнем носителе пользователь обязательно должен ввести PIN-код. В качестве внешнего носителя используются токены (электронные USB-ключи или смарт-карты). Данные, используемые для генерации ключа шифрования, размещаются в защищённой памяти токена и не могут быть прочитаны злоумышленником без знания им соответствующего PIN-кода (см. схему №3)

Утрата токена ещё не означает раскрытия самой информации. Для защиты от прямого подбора PIN-кода ставится аппаратная временная задержка между двумя последовательными попытками или аппаратное же ограничение на количество неправильных попыток ввода пин-кода (например, 15), после чего токен просто блокируется.

Поскольку токен может использоваться в разных приложениях, а PIN-код используется один и тот же, то можно обманным путём вынудить пользователя ввести свой PIN-код в подложной программе, после чего считать необходимые данные из закрытой области памяти токена. Некоторые приложения кэшируют значение PIN-кода в рамках одного сеанса работы, что так же несёт в себе определённый риск.


СХЕМА №3. ШИФРОВАНИЕ МАСТЕР-КЛЮЧА С ИСПОЛЬЗОВАНИЕМ ЗАЩИЩЕННОГО ВНЕШНЕГО НОСИТЕЛЯ (ТОКЕН, СМАРТ-КАРТА).

## ВАРИАНТ ЧЕТВЁРТЫЙ: СМЕШАННЫЙ

Возможен вариант, когда для генерации ключа шифрования одновременно используются пароль, ключевой файл на внешнем носителе и данные в защищённой памяти токена (см. схему №4).

Такой способ довольно сложен в повседневном использовании, поскольку требует от пользователя дополнительных действий. Многокомпонентная система также значительно сильнее подвержена рискам утраты доступа: достаточно потерять один из компонентов, и доступ без использования заранее созданной резервной копии уже не возможен.


СХЕМА №4. ШИФРОВАНИЕ МАСТЕР-КЛЮЧА С ИСПОЛЬЗОВАНИЕМ НЕСКОЛЬКИХ КОМПОНЕНТОВ.

## ВАРИАНТ ПЯТЫЙ: ОПТИМАЛЬНЫЙ

Отдельного рассмотрения заслуживает ещё один подход к организации безопасного хранения мастер-ключа, лишённый основных недостатков вышеперечисленных вариантов этот способ представляется наиболее оптимальным.

Современные токены (см. рис. № 1) 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.

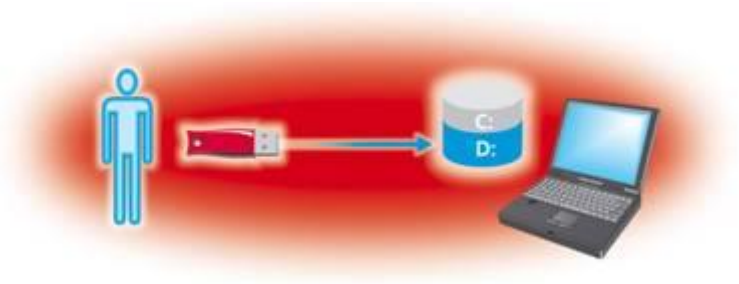


РИС. №1.СМАРТ-КАРТА И USB-КЛЮЧ, ЯВЛЯЮЩИЙСЯ ПОЛНОФУНКЦИОНАЛЬНОЙ СМАРТ-КАРТОЙ.

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 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 пин-код от неё. Затем мастер-ключ аппаратно расшифровывается с помощью закрытого ключа, хранящегося на смарт-карте, и пользователь получает доступ к данным.

Такой подход (см. схему №5) сочетает в себе безопасность и удобство использования.


СХЕМА №5. ШИФРОВАНИЕ МАСТЕР-КЛЮЧА С ИСПОЛЬЗОВАНИЕМ АСИММЕТРИЧНОГО АЛГОРИТМА ШИФРОВАНИЯ.

В вариантах 1, 2, 3 и 4 очень важным является выбор способа генерации ключа шифрования на основе пароля и/или данных с внешнего носителя. Уровень безопасности (в криптографическом смысле),

обеспечиваемый этим способом, должен быть не ниже, чем уровень безопасности остальных компонентов системы. Скажем, вариант, когда мастер-ключ просто хранится на внешнем носителе в инвертированном виде, крайне уязвим и небезопасен.

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.

Аппаратное ограничение на количество неправильных попыток ввода PIN-кода нивелирует риск его подбора и позволяет использовать достаточно простой для запоминания PIN-код.

Использование одного устройства с несложным PIN-кодом повышает удобство без ущерба для безопасности.

Создать дубликат смарт-карты не может даже сам пользователь, т.к. нет возможности скопировать закрытый ключ. Это также позволяет без опасения использовать смарт-карту совместно с любыми другими программами.

## ТЕХПОДДЕРЖКУ ВЫЗЫВАЛИ?

Есть и ещё один критерий выбора, который зачастую остаётся без внимания, но при этом относится к разряду «критических». Речь идёт о качестве технической поддержки.

Не вызывает сомнения, что защищаемая информация является ценной. Быть может, её утрата принесёт меньший вред, чем публичное раскрытие, но определённое неудобство будет доставлено в любом случае.

Оплачивая продукт, Вы, в том числе, платите и за то, что он будет нормально функционировать, а в случае сбоя Вам оперативно помогут разобраться в проблеме и устранить её.

Основная сложность заключается в том, что заранее оценить качество техподдержки довольно сложно. Ведь существенную роль служба техподдержки начинает играть на поздних стадиях внедрения, на этапе опытной эксплуатации и после завершения внедрения, в процессе сопровождения системы.

Критериями качества технической поддержки можно считать: время реакции на запрос, полноту ответов и компетентность специалистов. Рассмотрим их чуть более подробно.

Зачастую эквивалентом качества работы службы технической поддержки считается скорость реакции на запрос. Тем не менее, оперативные, но неправильные рекомендации могут принести значительно больший вред, чем простое их отсутствие.

Представляется разумным отдавать предпочтение российским разработкам или, по крайней мере, зарубежным фирмам, имеющим своё представительство в России. Разговаривая со специалистом на родном языке, Вы скорее поймёте друг друга.

Если продукт иностранный, то будьте готовы к возможным временным задержкам. Это может происходить потому, что Ваши вопросы будут переводиться на, например, английский, а ответы разработчика обратно на русский. Качество перевода оставим на совести специалистов техподдержки.

Условия оказания техподдержки обычно указаны на сайте. Вполне может оказаться, что эти условия для Вас неприемлемы: круглосуточной поддержки нет, а из-за разницы во времени у Вас есть один час в день, чтобы задать вопрос.

Списки частых вопросов (FAQ) могут стать источником дополнительной информации не только о самом продукте, но и о компетентности специалистов, работающих в компании. Например, отсутствие такого раздела наводит на мысли о непопулярности данного продукта или об отсутствии в организации отдельных

специалистов, занимающихся техподдержкой, способных написать базу знаний по обращениям пользователей. Забавно, но на некоторых сайтах в ответах на частые вопросы встречаются ошибки, в том числе и в написании названия самого продукта.

## ВЫХОЖУ ОДИН Я НА ДОРОГУ...

Мы кратко рассмотрели основные критерии, которые желательно учитывать при выборе системы шифрования данных. Вне всякого сомнения, такой выбор непрост из-за потенциально высокой цены ошибки. Именно поэтому к нему нужно подходить максимально ответственно. Помимо вышеперечисленного, нелишним будет обратить внимание ещё на несколько аспектов, таких как: авторитет и репутация производителя (косвенно можно оценить по количеству упоминаний в СМИ и популярности сайта компании), возможность интеграции продукта с другими средствами информационной безопасности (скажем, гораздо удобнее получать доступ к целому ряду информационных ресурсов с помощью одного токена, чем иметь «связку» устройств - на каждый случай свой), а также отзывы на независимых форумах пользователей шифро-систем.

Как видно, в процессе выбора можно зайти достаточно далеко. Наверняка у каждого найдутся свои собственные, важные именно для него, критерии сравнения. В конце-концов никто не запрещает сравнивать длительность гарантийных сроков, качество упаковки и соответствие цветовой гаммы бренда компании-производителя корпоративному стилю вашей организации. Главное – правильно расставить весовые коэффициенты.

В любом случае, прежде всего нужно трезво оценивать угрозы и критичность данных, а средства обеспечения безопасности желательно выбирать руководствуясь тем, насколько успешно они справляются со своей основной задачей – обеспечением защиты от несанкционированного доступа. В противном случае деньги лучше потратить на менеджер закачек.