Проанализировав результаты, полученные из таблиц 3 и 4, сделаем вывод, что стойкость блочных симметричных шифров напрямую зависит от длины блока. Алгоритмы SHACAL-1 и тем более SHACAL-2 полностью соответствуют по длине блока требованиям сегодняшнего дня.

VI Выводы

Проведя детальный анализ по стойкости SHACAL к наиболее мощным известным сегодня атакам, мы пришли к заключению, что линейная криптоаналитическая атака на SHA как функцию шифрования потребовала бы как минимум 2^{80} известных открытых текстов, а дифференциальная атака – как минимум 2^{116} выбранных открытых текстов. Заметим, что мы подробно рассмотрели конструктивные линейные приближения и дифференциальные характеристики. Очень может быть, что существуют другие приближения и характеристики на SHA-1, которые не обнаруживаются таким типом анализа. Вместо этого, они могли бы быть найдены с помощью атаки «грубой силы». Так как не существует известных приемов для такого поиска, то такая возможность должна рассматриваться как маловероятная настолько, что не представляет практического интереса.

Наши способы построения приближений и характеристик являются специальными, но базирующимися на значительном практическом опыте. Мы были очень осторожными в наших оценках и с большой вероятностью утверждали, что линейная или дифференциальная криптоаналитическая атака с использованием менее чем 2^{80} блоков открытого текста является невозможной. Мы отметили, что с этого места 160-битового блочного шифра начинается утечка информации открытого текста при использовании его для шифрования такого большого текста с тем же ключом.

И, наконец, мы упоминаем, что дополнительные криптоаналитические приемы, такие как линейные оболочки (hulls), многократные линейные приближения и разнообразные виды дифференциалов не способны внести какие-либо существенные отличия в наш анализ и оценки. И поэтому они не представляют никакого практического интереса для сделанных нами выводов.

Заключение

Для SHA-1 была обнаружена атака скольжения, что демонстрирует неожиданное свойство функции сжатия, но это — не угроза для нормального использования хэш-функции. Тем не менее, эта атака также указывает на слабость в ключевом планировании шифровального режима SHA-1. Атака скольжения на SHA-1 не распространяется на SHA-2, поскольку в SHA-2 в каждом шаге функции сжатия используется уникальная добавочная константа. Поэтому проект Nessie и выбрал алгоритм SHACAL-2 победителем и рекомендовал его для всестороннего применения в области криптографической защиты информации.

Литература: ***1.*** *National Institute of Standards and Technology, "New secure hash algorithms." 2000.* ***2.*** *National Institute of Standards and Technology, "FIPS-180-2: Secure Hash Standard (SHS)." Aug. 2002. Available at http://csrc.nist.gov/publications/jips/. [p. 76, 132, 137, 141, 142, 144]* ***3.*** *M-J. O. Saarinen, "Cryptanalysis of block ciphers based on SHA-1 and MDS. "In Proceedings of Fast Software Encryption {FSE'03 (T. Johansson, ed.), Lecture Notes in Computer Science, Springer-Verlag, 2003. Also available at http://www.tcs.hut.fi/~mjos/shaan.ps. [p. 75, 76, 77, 141]* ***4.*** *J. Kim, D. Moon, W. Lee, S. Hong, S. Lee, and S. Jung, "Amplified boomerang attack against reduced-round SHACAL." in Proceedings ofAsiacrypt'Q2 (Y. Zheng,ed.)$_f$ no. 2501 in Lecture Notes in Computer Science, pp. 243 (253, Springer-Verlag, 2002. Also in Proceedings of the Third NESSIE Workshop, 2002. [p. 76, 98, 140, 141]* ***5.*** *E. Biham, N. Keller, and O. Dunkelman, "Rectangle attacks on SHACAL-L "In Proceedings of Fast Software Encryption {FSE'03 (T. Johansson, ed.), Lecture Notes in Computer Science, Springer-Verlag, 2003. NES/DOC/TEC/WP5/031.fp. 76, 98, 141]*

УДК 621.391

ПРИМЕНЕНИЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СФЕРЕ БАНКОВСКИХ ТЕХНОЛОГИЙ

Вячеслав Татьянин
ООО «АВТОР»

Аннотация: **Даны рекомендации для правильного выбора систем защиты информации в сфере банковских технологий. Приведены примеры применения средств криптографической защиты информации.**

Summary: **Recommendations for a correct choice of systems of protection of the information in sphere of bank technologies are given. Examples of application of means of cryptographic protection of the information are resulted.**
Ключевые слова: **Защита информации, смарт-карта, криптографическая защита.**

Крупнейшие мировые производители операционных систем и прикладных программ большое внимание уделяют вопросу безопасности. С появлением очередных версий программного обеспечения наряду со значительным увеличением функциональных возможностей мы с большой радостью узнаем о тех или иных новшествах, повышающих стойкость систем и сетей к несанкционированному воздействию злоумышленников. Но проходит время, и мы узнаем о различных атаках на системы безопасности, недостатках программного обеспечения, способах получения несанкционированного доступа к информации. История развития систем защиты и их преодоления развивается по спирали: некоторое время уровень безопасности устраивает пользователя, впоследствии возникают угрозы, что требует усиления защиты, наступает некоторая стабильность... и вновь проблемы. Почему же так происходит? Новые криптографические алгоритмы, увеличение длины ключа, совершенствование протоколов управления и взаимодействия элементов системы, увеличение производительности компьютеров, казалось бы, должны решить все проблемы надолго и всерьез. Причин, конечно же, множество. В рамках одной статьи сложно дать общие рекомендации для правильного выбора систем защиты. Поэтому ограничимся некоторыми примерами.

I Защита информации в системе «Клиент-Банк»

В последние годы многие клиенты банка переходят на автоматизированное самообслуживание своих счетов. Преимущества этого сервиса очевидны (оперативность, экономия времени, сокращение транспортных расходов и прочее) и поэтому количество клиентов, решающих идти в ногу со временем, постоянно растет. Некоторые коммерческие банки обслуживают уже более тысячи таких клиентов. Тенденция к увеличению количества клиентов сохраняется, одновременно увеличивая проблемы безопасности. Кто может дать гарантию того, что очередным клиентом не окажется компьютерный мошенник?

Вопросы защиты информации, как правило, мало интересуют клиентов. Они полностью полагаются на службы защиты банков, что вполне закономерно, так как там работают квалифицированные специалисты по безопасности. При возникновении конфликта между банком и клиентом, ответственность за безопасность информации всегда лежит на банке — даже и в том случае, если арбитражный суд признает его правоту вследствие грамотно оформленного договора с клиентом (например, с учетом модели “взаимного доверия”). В подобной ситуации важнее “моральная”, а не юридическая ответственность банков — иначе итогом станет недоверие и потеря клиентов.

Проанализировав различные модели угроз в системах «Клиент-Банк», специалисты нашей фирмы пришли к однозначному выводу, что на уровне клиентов банка только аппаратные средства шифрования и цифровой подписи способны выполнять свою задачу. Пресловутые хакеры, как правило, не занимаются “взломом” алгоритмов — это очень сложный путь. Значительно проще и быстрее производить атаку на ключевую информацию или протоколы взаимодействия составных элементов системы защиты. А как можно надежно сохранить ключевую информацию при использовании программных средств защиты и защитить программу защиты от дизассемблирования?

В чем же принципиальное отличие аппаратных средств защиты? Для того чтобы получить ответ на этот вопрос необходимо понять отличия в принципах работы программ, работающих в персональном компьютере и в специальном устройстве.

Компьютер является универсальным средством и позволяет решать самые разнообразные задачи и приложения. Компьютеры относится к классу так называемых открытых систем: они разрешают пользователям вносить изменения в программное обеспечение или создавать новое. Программа в компьютере выполняется из оперативной памяти, которая загружается из внешнего накопителя информации во время непосредственного выполнения кода программы. Программист из всего огромного массива данных, находящихся в оперативной памяти, может выделить код выполняемой в настоящий момент программы. Его анализ, изменение и запуск модифицированного кода являются «открытыми воротами» для распространения вирусов. Поэтому вместо вопроса «Можно ли вскрыть программу?», правильнее будет задать следующий: «Сколько времени требуется для этого, какие предоставляются средства и какова цель работы?».

В отличие от компьютера специальные устройства предназначены для решения конкретных задач. Код программы выполняется, как правило, из постоянной памяти программ, ее невозможно изменить или заставить работать по-другому. Если правильно выбран процессор устройства, то код программы

гарантированно защищен от чтения. Даже такое дорогостоящее оборудование, как электронный микроскоп, который может сканировать поверхность кремниевой пластины чипа на уровне микронной технологии, для некоторых процессоров бессилен сосчитать код программы. Вскрытие специальных средств защиты возможно в случаях неправильного их проектирования, допущенных ошибок разработки программного обеспечения или размещения в коде программных закладок. Для исключения подобного, рекомендуется пользоваться услугами фирм, устойчиво работающих на данном рынке, а также применять сертифицированные устройства.

Для защиты информации в системе «КЛИЕНТ-БАНК» предлагаем использовать комплекс аппаратно-программных средств криптографической защиты информации **CryptoBank**. Предлагаемый комплекс является новейшим решением надежной защиты банковской информации с использованием смарт-карт технологий.

При разработке комплекса CryptoBank в первую очередь учитывался факт, что на уровне клиентов банка нет возможности использовать организационные мероприятия защиты. Поэтому все основные операции в системе защиты CryptoBank, связанные с защитой информации (шифрование, аутентификация, проверка полномочий, хранение и установка ключей, ведение протоколов), реализованы на аппаратном уровне с учетом современных новейших решений – смарт-карт технологий, высокопроизводительных защищенных процессоров сигналов. Программная часть системы защиты реализует второстепенные вспомогательные функции, такие, как тестирование, инициализация, интерфейс с прикладными задачами, съем протоколов и т. п. Такой подход к построению системы совместно с использованием криптографических алгоритмов, разрешенных для применения в Украине, обеспечивает гарантированную защиту обрабатываемых данных.

В отличие от существующих программных средств, в которых в качестве носителей ключей применяется дискета или TOUCH-Memory, предлагаемая система позволяет без каких-либо дополнительных организационных мер гарантированно защитить электронные банковские документы. В системе CryptoBank все криптографические операции выполняются аппаратными средствами, в которых носителем ключевой информации является смарт-карта. Операционная система смарт-карты гарантированно обеспечивает защиту информации от несанкционированного чтения, копирования и модификации, даже при потере носителя информации.

В качестве электронного носителя системы используется смарт-карта CryptoCard, представляющая собой микропроцессорную систему, имеющую высокую производительность и степень защищенности. Она непосредственно выполняет шифрование/дешифрование и формирование/проверку цифровой электронной подписи. Ключевая информация в CryptoCard записывается в момент ее эмиссии. При дальнейшей эксплуатации смарт-карты из нее невозможно прочитать эту информацию.

Международными финансовыми организациями формат электронной карты, соответствующий стандарту ISO7816, признан в качестве банковского стандарта. Банковский формат носителя ключей, в отличие от разнообразных "брелковых" форм, клиентам более удобен в хранении и использовании, а банкам позволяет значительно экономнее строить систему по одновременному обслуживанию большого количества карт, а также размещать служебную и рекламную информации.

В случае возникновения спорных ситуаций в вопросе отправки/приема электронных документов, система CryptoBank позволяет провести электронный арбитраж на основе анализа информации аппаратного и программного журналов. Протоколирование информации является важной арбитражной функцией системы CryptoBank. Протоколы ведутся в устройствах отправителя и получателя документов. Протокол, который ведется в аппаратуре, позволяет зафиксировать следующую информацию: дату и время обработки документа, идентификатор получателя/отправителя документа, значение счетчика обращений к устройству, код аутентификации (цифровая подпись) документа. Программный протокол дополнительно фиксирует копию электронного документа, которая при необходимости может шифроваться. Код аутентификации (цифровая подпись) вычисляется на все поля протокола. Устройства позволяют фиксировать несколько десятков тысяч записей протоколов. При возникновении конфликтной ситуации для выполнения арбитража производится сравнение программных и аппаратных протоколов отправляющей и принимающей стороны.

Аппаратный счетчик каждый раз при обращении к устройству увеличивает свое значение на единицу. Извне он никогда не может быть изменен или обнулен. Значение счетчика позволяет нумеровать обращения к устройству. Кроме этого, значение счетчика может быть использовано в тех случаях, когда не ведется аппаратный протокол. В этом случае при добавлении новой записи в программный протокол производится проверка целостности последней записи протокола и сравнение значений счетчиков. В случае нарушения целостности или несовпадения кодов счетчиков, устройство информирует пользователя и не разрешает выполнять последующую операцию.

Удаленное управление устройствами выполняет программно-аппаратный комплекс CryptoNet, который формирует защищенные криптографическими методами команды управления: добавить связь, удалить связь,

сменить ключ, прочитать протокол, очистить протокол и др.

Новая система защиты позволяет снизить уровень организационных ограничений, присущих программным средствам защиты (требования по хранению носителя ключа, к выполняемым задачам и доступу к компьютеру с установленным АРМ "КЛИЕНТа" и др.).

Система поставляется в комплекте с пользовательским интерфейсом (API), что позволяет легко ее встраивать в программное обеспечение автоматизированных рабочих мест и существующие Windows-приложения (Microsoft Word, Microsoft Explorer, Microsoft Outlook Express, Microsoft Exchange, IBM Lotus 5 и др.). Особенностью системы является комплексный подход к решению многих задач защиты информации, реализуемых с помощью системно совместимых устройств, что позволяет поэтапно, минимизируя затраты, реализовывать функции защиты, доступа и разграничения полномочий. Широкий набор аппаратных средств, отличающихся между собой производительностью и способом подключения к ПЭВМ, позволяет экономично организовать систему защиты на всех уровнях (банк, филиал, отделение банка, клиенты с большим и малым оборотом средств). Программное обеспечение на уровне драйверов обеспечивает работу всех типов устройств с различными интерфейсами (ISA, PCI, RS-232, USB) с общим пользовательским интерфейсом (API).

Состав системы криптографической защиты информации CryptoBank:

- *Комплекс управления, арбитража и генерации ключевой информации CryptoNET-300 – предназначен для ведения баз данных, генерации ключей, эмиссии карточек, удаленного управление устройствами КЗИ, учета технических средств, выполнения арбитражных функции.*
- *Устройства криптографической защиты информации – CryptoLine-345 PCI, CryptoLine-335 PCI, CryptoLine-325 USB, смарт-карта CryptoCard.*
- *Дополнительное оборудование: карт-ридер USB, карт-ридер RS-232*

Хотя достоинства аппаратных устройств защиты очевидны, многих может смутить цена. Поэтому для клиентов банка, у которых оборот платежных поручений невелик, до 500 платежных поручений в день, на базе смарт-карты с операционной системой UKRCOS разработано приложение **CryptoCard**. CryptoCard по функциональным возможностям и форматам полей совместимо с устройствами CryptoLine. Главное отличие состоит в том, что все операции по обработке документов (включая криптографические) выполняются внутри смарт-карты. Электронный документ для обработки целиком передается в смарт-карту.

CryptoCard может поддерживать одновременную работу двух приложений: главного бухгалтера и директора. CryptoCard позволяет вести внутри карты протокол до 1 тысячи записей.

На смарт-карте CryptoCard реализованы генератор псевдослучайных чисел, счетчик обращений, криптографические алгоритмы (по выбору пользователя): ГОСТ 28147-89, DES, Triple DES, которые обеспечивают следующую производительность (с учетом пересылки данных):

- скорость шифрования/дешифрования документов (в соответствии с ГОСТ 28147-89) — до 1 Кбайт/с;
- скорость вычисления кода аутентификации (MAC) — до 2 Кбайт/с;
- скорость одновременного шифрования и вычисления MAC — до 800 байт/с.

Для работы со смарт-картой CryptoCard требуется стандартный считыватель смарт-карт, соответствующий ISO 7816-3 (протокол T=1).

II Защита информации от несанкционированного доступа

А как должна вести себя система защиты в случае несанкционированного воздействия на нее со стороны администратора или сотрудников банка?

Система защиты должна быть защищена от копирования, устойчива к воздействию вирусов. В случае возникновения спорных моментов система защиты должна обеспечивать арбитражные функции. Программные средства защиты не позволяют надежно решить ни одну из этих задач. В то же время аппаратными средствами невозможно комплексно решить все вопросы автоматизации, так как большая часть операций по обработке данных, не связанных с защитой, выполняется программно. В момент передачи данных в криптографическое устройство вирус может воздействовать на данные и исказить их. Устройство, используя арбитражные функции, может определить факт несанкционированного воздействия, но предотвратить само воздействие не в состоянии. Для некоторых систем арбитражная функция может оказаться недостаточно сдерживающим фактором.

Хорошим и относительно недорогим средством для решения задач защиты информации от несанкционированного доступа (НСД), являются программно-аппаратный комплекс **CryptoGuard**, который начинает выполнение своих функций еще в момент начальной работы BIOS компьютера, до загрузки операционной системы. Система защиты разрешает запустить операционную систему только после предъявления зарегистрированной смарт-карты и ввода пароля, блокируя тем самым несанкционированное включение компьютера. После идентификации пользователя производится проверка целостности файлов

операционной системы, запускаемых приложений, MBR (Master Boot Record), BR (Boot Record) и ключей Registry. После загрузки операционной системы устанавливаются драйвера защиты, которые являются связующим элементом между BIOS и операционной системой и непосредственно управляют механизмами защиты. До момента инициализации драйверов защиты клавиатура и порт мыши блокируются, что не позволяет нарушить последовательность загрузки операционной системы и проверку целостности ключевых элементов системы.

В состав системы защиты CryptoGuard входят:

- АРМ администратора системы безопасности CryptoNet (сетевая версия и для автономной рабочей станции);
- устройства системы защиты (PCI, USB, RS-232), устанавливаемые непосредственно на рабочих местах пользователей;
- программное обеспечение устройств защиты;
- електронные карты.
- АРМ администратора системы безопасности CryptoNet позволяет дистанционно:
  - оперативно менять профиль (права доступа) пользователя;
  - собирать журналы работы пользователей и вести их обработку;
  - осуществлять мониторинг и, при необходимости, останавливать процессы (задачи) на компьютере пользователя;
  - посылать сообщения пользователям и принимать сообщения от системы защиты на компьютере администратора.

При необходимости компьютер пользователя может быть дистанционно блокирован (блокируются клавиатура, мышка и гасится экран дисплея) без остановки загруженных приложений. Разблокирование производится по команде из CryptoNet, либо карточкой пользователя.

Система CryptoGuard обеспечивает защиту информации от НСД и позволяет разграничивать доступ к сетевым ресурсам практически для всех типов сетей поддерживаемых операционными системами (ОС): Windows 9x, Windows NT 4.0, Windows 2000, Windows XP и многих клонах Unix, а также в DOS, Novell.

Нередко подобные системы защиты преодолеваются простым извлечением устройств защиты из компьютера. Но если организационные меры так слабы, что пользователям удается открывать компьютеры, то они могут извлечь из него и винчестер – источник всей информации. Для защиты от несанкционированных действий подобного рода система CryptoGard может работать в режиме прозрачного шифрования, который позволяет хранить информацию на внешних носителях (винчестер, дискета, ZIP, MO) в зашифрованном виде. При обращении к зашифрованным данным драйвер «на лету» выполняет их дешифрование, предоставляя приложению открытую информацию. Аналогичный принцип реализован при передаче информации по сетям с протоколом TCP/IP. В списке указываются адреса (IP) абонентов, с которыми обмен информацией должен происходит в зашифрованном виде. При необходимости, для обеспечения целостности документов и аутентификации абонентов, эта информация может подписываться. Система защиты позволяет контролировать обмен TCP/IP пакетами на уровне максимально приближенном к драйверу сетевых плат, что обеспечивает универсальность и повышенный контроль над прохождением пакетов. По желанию администратора доступ к адресатам или от них протоколируется. При этом есть возможность протоколировать как разрешенные, так и запрещенные попытки доступа, а также дату, время, тип и название приложений, с помощью которых производился доступ. Это позволяет запретить доступ пользователя к нежелательным TCP/IP адресам и предотвратить несанкционированный доступ извне.

Система CryptoGard по форматам и протоколам обмена совместима с автоматизированной системой пропусков и доступа к объектам **CryptoLock**. Совместное их использование позволяет комплексно решить задачи санкционированного доступа в закрытые зоны (парковка, здания, помещения, сети, компьютеры, файлы), причем использование одних и тех же смарт-карт и комплексов управления в обеих системах позволяет существенно сократить расходы и улучшить сервис обслуживания.

III Смарт-карты

Основным элементом любой системы защиты является ключевая информация. От того, как построена подсистема хранения и распределения ключей во многом зависит безопасность и стойкость системы. Известные способы хранения ключей с использованием перфокарт, дискет, магнитных карт, электронных карт памяти (Memory card), Touch-memory имеют главный недостаток – хранимая в них информация может быть прочитана с помощью специальных, относительно недорогих средств и в относительно небольшие сроки. Эти носители ключей легко копируются, подделываются и эмулируются. Единственно надежным способом защитить ключи, находящиеся на внешнем носителе, является использование криптографических

методов, которые выполняются микроконтроллером, встроенным в защищаемую память. Данный тип носителей ключей относится к классу микропроцессорных карт (Smart card).

С английского языка смарт-карта переводится как интеллектуальная. В нашем лексиконе за ней закрепилось также название микропроцессорная.

Кристалл для смарт-карты (рис.1) в базовой конфигурации состоит из центрального процессора (CPU), однократно программируемой памяти (ROM), оперативной памяти (RAM), энергонезависимой электрически перепрограммированной памяти (EEPROM), секретной логики (Security Logic), интерфейса ввода/вывода информации (I/O).

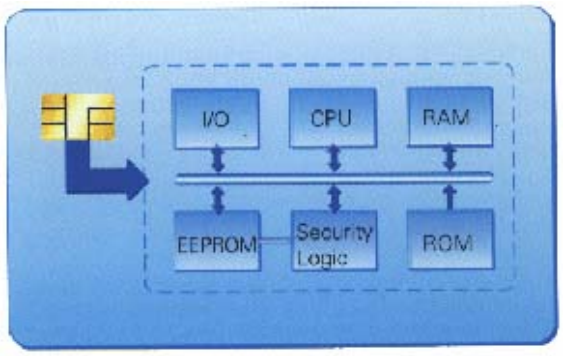

Рисунок 1 — Кристалл для смарт-карты

Микропроцессор является сердцем кристалла. Он обеспечивает управление всеми элементами периферии, выполняет вычислительные операции и криптографические преобразования. Мозг карточки - память программы, которая определяет интеллект карточки и заставляет процессор функционировать по заданным правилам. Память программы находится в области ROM и программируется на заводе изготовителем кристаллов, а данный процесс называется маскированием кристалла. Он связан с технологическими операциями по изготовлению кремниевых пластин, поэтому стоит очень дорого. Маскирование экономически целесообразно выполнять при заказах в несколько нескольких сотен тысяч кристаллов. Программа смарт-карты создается в форме операционной системы. Это обеспечивает гибкость в применении, позволяет создавать универсальные средства для многих приложений пользователей и гарантирует независимость от разработчиков операционных систем при создании собственных приложений. Карточная операционная система функционально похожа на операционную систему компьютера: имеет файловую организацию данных, защищает их от несанкционированного доступа, разграничивая права пользователей, управляет интерфейсами обмена и собственной периферией (EEPROM, таймер, генератор шума, датчики и прочее), позволяет запускать приложения пользователя, выполняет команды операционной системы и сервисные функции. Основные требования к операционной системе изложены в международном стандарте ISO7816, часть 4. Кроме основного назначения, память EEPROM позволяет поместить часть выполняемого кода программ. Это дает возможность программировать нестандартные приложения без дорогостоящей операции маскирования. Однако необходимо учитывать, что размер памяти EEPROM существенно влияет на стоимость кристалла. Поэтому для крупных проектов, код специального приложения целесообразно переводить в область памяти ROM. Эту операцию, как правило, выполняют поэтапно.

Последние достижения в технологии производства кристаллов позволяют в чипе прежних размеров дополнительно размещать криптопроцессоры Triple DES, RSA и элиптических кривых, таймер, порт UART, модуль подсчета CRC, генераторы случайного шума, дополнительную оперативную память, одновременно два интерфейса ввода/вывода – контактный и бесконтактный, а также увеличивать разрядность процессоров с 8 бит до 16 бит, размеры памяти ROM – до 64 Кбайт, EEPROM – до 32 Кбайт.

Микропроцессорный чип имеет несколько уровней защиты от несанкционированного доступа к хранимой в нем информации: программный, аппаратный, технологический.

Программный уровень реализуется средствами операционной системы, которые используют следующие способы и методы защиты:

- назначение индивидуальных атрибутов файлов;
- назначение индивидуальных прав доступа к файлам;
- доступ к файлам по заранее заданным правилам (проверка ПИН-кода и аутентификация);
- блокировка файлов, каталогов или карточки;

- защита ПИН-кодом отдельных файлов;
- противодействие подбору ПИН-кодов;
- счетчик попыток подбора ПИН-кодов;
- взаимная аутентификация между карточкой и терминалом;
- шифрование команд и данных;
- шифрование внутренних данных;
- шифрование канала обмена карточки с терминалом;
- использование сеансовых ключей для всех криптографических преобразований;
- защита от несанкционированного и непредусмотренного использования файлов.

Аппаратный уровень защиты поддерживается ресурсом кристалла, спроектированным изготовителем. Для этого в кристалле реализуются специальные датчики, устройства и элементы:

- детектор пониженного и повышенного напряжения питания;
- детектор пониженной и повышенной тактовой частоты;
- детектор пониженной и повышенной температуры;
- стирание области RAM при сбросе или срабатывании датчиков;
- самотестирование структуры чипа;
- защита от высокочастотных помех;
- генератор случайных тактов ожидания;
- скремблирование внутренних шин;
- прозрачное шифрование RAM, ROM, EEPROM;
- аппаратная защита чтения областей ROM, EEPROM, PROM;
- уникальный идентификационный номер кристалла;
- защита от использования в нештатных режимах работы;
- защита от накопления статистических данных по времени выполнения команд и энергопотреблению;
- уникальные характеристики шифрования или скремблирования внутренних RAM и EEPROM;
- защита от подключений зондами.

На различных стадиях производства кристаллов применяются технологические приемы, затрудняющие воссоздание структуры чипа и получение секретной информации. Создаются многослойные структуры кристаллов (до 22 слоев), ответственные части схемы (ROM и EEPROM) помещаются во внутрь, вводятся дополнительные слои металлизации. Внутренняя напряженность и внешняя металлизация защищают кристалл от оптического и электронного сканирования, обеспечивая его разрушение при послойном спиливании. Отсутствие общей шины и перемешивание структуры функциональных блоков (CPU, RAM, ROM и EEPROM) создают большие трудности при определении структуры чипа.

Совокупность применяемых программных, аппаратных и технологических мер ограничения доступа, а также криптографическая защита информации с использованием алгоритмов гарантированной стойкости исключают возможность получения доступа к данным, хранящимся на смарт-карте, гарантированно защищают электронную карту от копирования, эмуляции и несанкционированного повторного применения.

Область применения смарт-карт многогранна: банковские, предоплаченные, корпоративные, медицинские, дисконтные, игровые сервисные и клубные карты; транспортные проездные билеты; талоны авто заправок; карточки мобильной связи, платных дорог, парковок и телевидения; носители данных и ключевой информации; устройства шифрования и формирования цифровой подписи; идентификаторы, элементы доступа, электронные пропуска и прочее.

IV Защита речевой информации и данных

Основным способом подслушивания телефонных разговоров является подключение к каналу связи специальных устройств: регистраторов, магнитофонов, аппаратов прослушивания и пр. В настоящее время для закрытия речевой информации используются аналоговые и цифровые методы.

Аналоговые методы закрытия базируются на преобразовании частотно-временных параметров речевого сигнала. Системы, использующие аналоговые методы, часто называют речевыми скремблерами. Известно, что аналоговые методы закрытия речевой информации не могут обеспечить высокую стойкость закрытых сообщений и скремблеры, реализующие эти методы, относятся к системам с временной стойкостью.

В цифровых системах закрытия производится преобразование речевого сигнала или его параметров в цифровой поток, который шифруется выбранным алгоритмом и передается по каналу связи. Стойкость таких систем определяется стойкостью криптографического алгоритма.

Устройство **VDCrypt** реализует цифровые методы и предназначено для криптографической защиты речевой информации и данных. Функционально устройство состоит из трех основных элементов: модуля

сжатия речевой информации, который преобразует речевые сигналы в поток битов, модуля криптозащиты и модема, который обеспечивает передачу и прием закрытой информации по стандартному телефонному каналу связи (со скоростью до 14400 бит/сек.) Все три модуля реализованы в одном сигнальном процессоре, в целочисленной арифметике, что обеспечивает высокую надежность, гарантированную стойкость и относительно невысокую стоимость устройства.

Модуль сжатия речевой информации содержит аналоговый интерфейс, компандер, эхо компенсатор речевого тракта, вокодер и обнаружитель активности речи.

Аналоговый интерфейс согласует параметры телефонного аппарата с устройством VDCrypt, фильтрует аналоговый сигнал и обеспечивает его аналого-цифровое и цифро-аналоговое преобразование с частотой дискретизации 8 кГц с квантованием 16 бит на отсчет.

Компандер сжимает на 20 дБ динамический диапазон сигнала от микрофона телефонного аппарата и расширяет его на 14...26 дБ перед выдачей сигнала на телефонный капсюль трубки.

Эхо компенсатор обеспечивает разделение тракта приема и передачи при двухпроводном подключении телефонного аппарата к устройству VDCrypt. Уровень подавления составляет не менее 42 дБ.

Вокодер разработан на базе метода алгебраического линейного предсказания с кодовым возбуждением (ACELP). Для кодирования параметров линейного предсказания используется их представление в форме линейных спектральных частот. Для ослабления влияния ошибок в канале связи на качество принятой речи предусмотрена интерполяция параметров речи на искаженных фрагментах. Вокодер работает устойчиво при вероятности ошибки в тракте приема/передачи 10^{-2}. Вокодер обеспечивает натуральность звучания и узнаваемость говорящего. Речевой сигнал на выходе декодера по качеству мало отличается от сигнала на входе кодера. Алгоритм кодирования и декодирования речевого сигнала разработан специалистами киевской фирмы “VIMAS Technologies”.

Активность говорящего абонента во время телефонного разговора по среднестатистическим данным составляет 30-40 % времени. Остальное время занимают паузы общего разговора и прослушивания собеседника. Свободный ресурс может быть использован модемом для передачи данных от компьютера (через интерфейс USB). В режиме одновременной передачи речевой информации и данных обнаружитель активности речи производит автоматическое переключение модема с голоса на данные. Обнаружитель активности речи также используется в полудуплексном режиме работы модема для переключения трактов приема и передачи. Модем переходит в данный режим при ухудшении параметров канала связи.

Модуль криптозащиты позволяет в режиме реального времени шифровать/дешифровать данные, которые поступают от модуля сжатия и модема. Для шифрования используется криптографический алгоритм ГОСТ 28147-89 в режиме гаммирования без обратной связи. Для перехода в режим защищенной связи необходимо одному из абонентов нажать кнопку на передней панели устройства VDCrypt. В то время, когда модемы устанавливают связь (0,8...2 сек), модуль криптозащиты выполняет идентификацию абонентов, считывание ключевой информации со смарт-карты и выработку сеансовых ключей шифрования и дешифрования. Длина сеансовых ключей — 256 бит. Идентификация абонента производится путем сравнения полученного идентификационного поля со списком идентификационный полей, который хранится в смарт-карте, причем, сравнение этих полей выполняет смарт-карта. Режим защищенной связи может быть установлен только при положительной идентификации абонентов.

Пользователи устройств могут самостоятельно производить генерацию ключевой информации и записывать ее в смарт-карты, используя программно-аппаратный комплекс управления CryptoNet-700, который выполняет: конфигурирование сети абонентов, накопление и обслуживание данных о составе и состоянии сети абонентов. Комплекс управления ведет списки сети отдельно для абонентов, устройств и смарт-карт. Он может оперативно менять конфигурацию сети. К изменяемым параметрам сети относятся списки разрешенных корреспондентов каждого абонента, а также параметры, которые определяют функциональность и режим работы устройства.

Модем позволяет одновременно передавать речевые сообщения и данные по каналам связи: внутригородским коммутируемым или выделенным линиям телефонных сетей (общего пользования или ведомственных); междугородным и международным коммутируемым каналам телефонного типа; физическим линиям; УКВ радиосетям и радиолиниям. Для передачи данных в устройстве VDCrypt реализован интерфейс USB.

Особенностями модема являются: малое время вхождения в связь (в пределах 0,8...2 сек.), устойчивость синхронизации и быстрое ее восстановление (как правило, не более 1 сек.) и возможность работы с каналами связи низкого качества.

Нелинейный эхо компенсатор и корректор АЧХ уменьшают уровень шумов приемного тракта в дуплексном режиме. Для повышения устойчивости к помехам данные кодируются решетчатым кодом и

декодируются декодером Витерби. Высокое качество и скорость адаптации к частотным характеристикам канала связи достигается применением алгоритма Калмана. Влияние нелинейностей канала связи уменьшается за счет адаптации уровня и спектра линейного сигнала передатчика. Для выбора скорости и режима работы (дуплекс/полудуплекс), модем использует результаты оценки (измерения) параметров канала связи и информацию, полученную от модема корреспондента. Модем работает устойчиво при отношении сигнал/шум не менее 9 дБ.

V Заключение

Выбор системы защиты – чрезвычайно ответственный момент, поэтому должен осуществляться индивидуально при решении конкретной задачи. Необходимо учесть множество факторов воздействия на систему, составить модель предполагаемых угроз, оценить масштабы возможных потерь, сравнить их со стоимостью системы Правильный выбор системы защиты обеспечит целостность информации, безопасность самой системы в период ее эксплуатации, позволит продлить ее жизнь и, в конечном итоге, сократить расходы на нее.

УДК 004.73.004(045)

КОНТРОЛЬ ВІДПОВІДНОСТІ ОБЛАДНАННЯ МЕРЕЖ АСИНХРОННОГО РЕЖИМУ ПЕРЕДАЧІ

Олександр Сухопара
Національний авіаційний університет

Анотація: **Здійснено вибір показників ефективності використання АТМ-обладнанням ресурсів мережі передачі даних за функціональним призначенням, що має суттєвий практичний інтерес у зв'язку з широким застосуванням цього обладнання в сучасних глобальних транспортних мережах.**
Summary: **The selection of conformance parameters of ATM-equipment is executed that has essential practical interest in connection with wide application of this equipment in modern global transport networks.**
Ключові слова: **Технічна експлуатація, контроль відповідності, мережі передачі даних.**

I Вступ

Внаслідок високого динамізму розвитку сучасних технологій передавання даних відповідні технології технічного обслуговування сучасного обладнання глобальних транспортних мереж передачі даних (ПД) істотно відстають від реальних потреб практики. Тобто, самі мережі впроваджуються дуже швидкими темпами, у тому числі і в Україні, а от створення необхідних експлуатаційних документів, зокрема правил експлуатації або регламентів обслуговування мережного обладнання, затягується в часі з усіма негативними наслідками, що звідси випливають. На жаль, відсутні не тільки відповідним чином опрацьовані експлуатаційні документи в цій сфері, але навіть не отримані необхідні теоретичні моделі, що могли б бути основою для розробки таких документів. Особливо це стосується проблем технічного обслуговування обладнання, що функціонує відповідно до специфікацій технології асинхронного режиму передачі (Asynchronous Transfer Mode – ATM). Зокрема, у відомих автору публікаціях майже відсутня інформація щодо показників відповідності, якими доцільно користуватися в процесах контролю працездатності такого обладнання. Слід зазначити, що ефективність системи технічної експлуатації (ТЕ) обладнання мереж ПД впливає на захищеність інформаційних ресурсів цих мереж, зокрема, сприяє протидії порушенням доступності інформації, що циркулює в каналах АТМ-мереж. Тому вибір показників відповідності для обладнання АТМ має суттєвий практичний інтерес.

II Постановка задачі

Автором даної статті здійснене обґрунтування вибору показників ефективності використання АТМ-обладнанням ресурсів мережі передачі даних за функціональним призначенням, які можуть використовуватися в процесах контролю відповідності обладнання мереж АТМ.

З метою отримання відповіді на питання, чи знаходиться обладнання АТМ або певна частина цього обладнання у працездатному стані, чи функціонує воно відповідно до вимог документів, які регламентують потоки процесів ТЕ мереж ПД, і чи здатне це обладнання до взаємодії з іншими частинами