СРЕДСТВА И РЕШЕНИЯ

ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сергей ПАНАСЕНКО
заместитель генерального директора ООО Фирма «АНКАД», к. т. н.

Новые информационные технологии позволяют расширить комплекс банковских услуг. Но, расширяя горизонты своего бизнес-предложения, банки получают и дополнительные риски, связанные, в том числе, с выполнением требований регуляторов и с угрозами безопасности. А ведь именно банк должен обеспечивать своими силами и средствами безопасность банковских операций, охрану имущества, защиту информации и информационной инфраструктуры и т.д. Требования о принятии банками мер защиты своего имущества и инфраструктуры содержатся в ряде федеральных законов и нормативных актов Банка России. Непродуманное с точки зрения безопасности использование новых технологий может привести к возникновению новых уязвимостей в столь критичном вопросе, как финансы.

На фоне последних мировых событий и экономических санкций, введенных западными странами в отношении России, наметилась четкая тенденция к снижению импортозависимости и в банковской сфере, в качестве примера чему можно привести переход на национальную систему платежных карт. Это, соответственно, предъявляет дополнительные требования к надежности и безопасности, а также к доверенному происхождению как аппаратной, так и программной составляющей всей информационной системы банков.

Для обеспечения надежной и безопасной обработки и передачи данных российская Фирма «АНКАД» предлагает широкую линейку продуктов под торговой маркой «КРИПТОН» («Crypton»), которая хорошо известна в России и за ее пределами. Это инновационные продукты, защищенные российскими патентами, созданные на основе отечественных криптоалгоритмов и соответствующие самым высоким требованиям стандартов и системы сертификации ФСБ и ФСТЭК России. Рассмотрим некоторые из них.

МОДУЛИ ДОВЕРЕННОЙ ЗАГРУЗКИ С УДАЛЕННЫМ УПРАВЛЕНИЕМ

Классическое назначение аппаратно-программных модулей доверенной загрузки состоит в идентификации и аутентификации пользователей, обеспечении контроля и разграничения доступа к вычислительным системам и их ресурсам, а также в контроле целостности используемой программной среды. Но, помимо этого, АПМДЗ семейства «КРИПТОН-ЗАМОК» можно рассматривать как аппаратный модуль обеспечения безопасности вычислительных средств в целом, поскольку на базе АПМДЗ могут быть построены комплексные решения по обеспечению информационной безопасности, в рамках которых модуль может выполнять различные дополнительные функции, в частности:

- создание различных контуров защиты;
- разграничение доступа к компьютерным сетям;
- управление сетевыми шифраторами;
- управление проходными шифраторами жестких дисков и USB-носителей;
- взаимодействие с программными средствами для обеспечения сквозной аутентификации пользователей и непрерывной защиты информации.

Модульная структура изделий «КРИПТОН-ЗАМОК» позволяет настраивать и дорабатывать их под конкретные требования, благодаря чему возможно построение многоуровневых решений по обеспечению информационной безопасности, адаптированных для различных информационных систем.

Кроме того, АПМДЗ данного семейства поддерживают возможность удаленного управления, что позволяет настраивать конкретные экземпляры модулей, учетные записи пользователей, профили защиты и прочие параметры этой распределенной (в т.ч. географически) системы обеспечения информационной безопасности с центрального рабочего места администратора по безопасности. Это значительно упрощает администрирование, позволяет вести мониторинг всей системы в реальном времени, а также снижает требования к квалификации персонала на местах, что также немаловажно.

АППАРАТНЫЕ СРЕДСТВА ШИФРОВАНИЯ

Основным методом обеспечения конфиденциальности банковских данных при их хранении или передаче по компьютерным сетям является шифрование. Причем именно аппаратное шифрование обеспечивает наиболее качественный уровень защиты за счет ряда факторов, основными из которых можно считать следующие:

- ключи шифрования обычно вводятся напрямую в аппаратный шифратор и не покидают его во время работы шифратора (т.е. не попадают в оперативную память или в системные шины компьютера), что делает практически невозможным перехват ключей злоумышленником;
- аппаратная реализация алгоритма шифрования гарантирует его неизменность, что не позволяет злоумышленнику вмешиваться в процесс шифрования с целью раскрытия и хищения данных.

Фирма «АНКАД» предлагает линейку аппаратных шифраторов, реализующих отечественные криптостандарты, включающую в себя следующие устройства:

- абонентские шифраторы, выполняющие операции шифрования и контроля целостности блоков данных по запросам прикладного программного обеспечения;
- проходные сетевые шифраторы «КРИПТОН AncNet», обеспечивающие защиту каналов передачи данных путем шифрования информационных полей IP-пакетов и выполнения ряда дополнительных функций по противодействию сетевым угрозам безопасности;
- проходные шифраторы жестких дисков «КРИПТОН-ПШД» и проходные шифраторы жестких и флэш-дисков «КРИПТОН-Интеграл» позволяют в автоматическом режиме шифровать данные на жестких дисках компьютера и съемных USB-носителях.

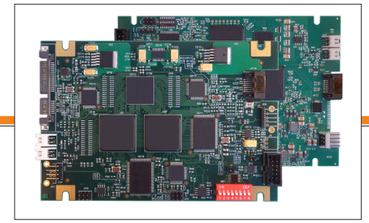
Все перечисленные выше аппаратные шифраторы выполнены в соответствии с наиболее строгими требованиями системы сертификации ФСБ и позволяют защищать не только коммерческую тайну, но и информацию, составляющую государственную тайну, в т.ч. с высокими грифами секретности.

Как было сказано выше, шифраторы могут работать в связке с АПМДЗ «КРИПТОН-ЗАМОК» (но могут работать и автономно) в рамках построения интегрированных систем защиты информации.

СТРОГО ОДНОНАПРАВЛЕННАЯ ПЕРЕДАЧА ДАННЫХ

Множество угроз безопасности информации проистекает благодаря наличию двусторонней связи между системами, обрабатывающими критически важную информацию, и общедоступными компьютерными сетями. В этом случае обычно применяются многоуровневые и эффективные средства защиты, но само наличие подобных соединений оставляет внешнему злоумышленнику потенциальные возможности атаки на защищаемые внутренние сети, а инсайдеру — возможности компрометации данных, составляющих коммерческую тайну.

Система однонаправленной связи позволяет выполнять строго однонаправленную передачу данных из сети менее строгой в сеть более строгой категории. Данная система основана на сетевых адаптерах DIOD, которые имеют только один оптический сетевой разъем — только приемный или только передающий. Благодаря этому, обратная передача данных в сеть менее строгой категории физически невозможна. Для передачи данных между адаптерами DIOD используется значительная избыточность с контролем целостности.



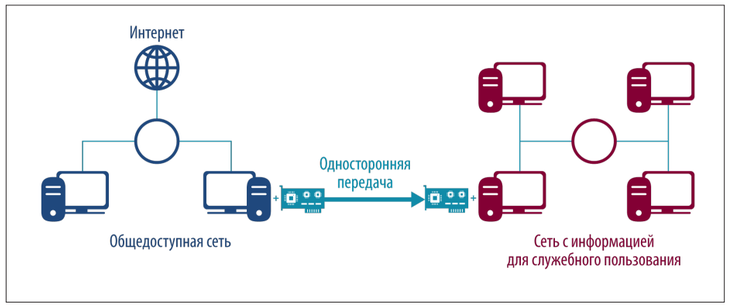
Проходные шифраторы «КРИПТОН-Интеграл» и «КРИПТОН-ПШД»

Таким образом, существует возможность вноса и обработки данных из внешних компьютерных сетей во внутренние, но гарантированно невозможна утечка данных из защищаемых сетей посредством сетевого интерфейса. Отмечу, что устройства DIOD могут использоваться каскадно между сетями с нарастающим уровнем значимости данных.

АРХИТЕКТУРА ЗАЩИЩЕННОГО «ТОНКОГО КЛИЕНТА»

Основная идея терминальных решений восходит к эпохе больших ЭВМ и сводится к тому, что вся обработка информации происходит на централизованных серверах, а на конечных рабочих местах она лишь отображается на экране.

В связи с этим существуют определенные преимущества использования «тонкого клиента» применительно к компьютерным системам, обрабатывающим информацию с повы-



Организация односторонней передачи данных

шенными требованиями к ее защите, в частности:

- вся информация физически хранится и обрабатывается только на выделенных серверах, которые можно защитить организационными мерами, что чрезвычайно важно для офисов обслуживания клиентов банков;
- отсутствует информация на терминалах пользователей в выключенном состоянии, что не позволит злоумышленнику воспользоваться компьютером в отсутствие персонала;
- архитектура «тонкого клиента» может быть легко адаптирована для использования в географически распределенных средах;
- существует возможность жесткого контроля информационных потоков в системе;
- администрирование и обновление системы могут выполняться централизованно — например, из головного офиса банка;
- есть возможность организации полного мониторинга действий сотрудников и управления системой в режиме реального времени.

Таким образом, использование терминальной архитектуры позволяет решить многие проблемы, присущие классическим сетевым архитектурам, и заметно повысить уровень безопасности и надежности информационных систем.

Архитектура защищенного «тонкого клиента» позволяет обеспечить дальнейшее поэтапное усиление степени защиты информационных систем. Усиление безопасности может, в частности, производиться по следующим направлениям:

1. Обеспечение защиты от несанкционированного доступа и доверенный запуск серверов за счет их оснащения аппаратно-программными модулями доверенной загрузки «КРИПТОН-ЗАМОК».

2. Организация единой многофакторной идентификации и аутентификации пользователей.

3. Обеспечение централизованного хранения информации о субъектах и объектах системы, правил разграничения доступа и прочих настроек системы и ее отдельных компонентов. Это позволяет гибко управлять правами доступа и параметрами пользователей, а также мгновенно распространять изменения на всю систему. Вся указанная информация может храниться на выделенном сервере баз данных с организацией доступа к ней только через специальный сервер защиты и управления терминалами, осуществляющий авторизацию всех запросов к данным.

4. Выполнение доверенной загрузки рабочей операционной системы терминала с сервера в среде АПМДЗ только после успешной аутентификации пользователя. Поскольку операционная система загружается в оперативную память терминала, она уничтожается после выключения питания терминала, что позволяет избежать угрозы модификации или несанкционированного доступа к терминальной ОС.

5. Разграничение доступа к объектам файловой системы серверов с помощью программной системы контроля и разграничения доступа «КРИПТОН-ЩИТ», интегрированной с АПМДЗ «КРИПТОН-ЗАМОК».

6. Аппаратное шифрование передаваемой по сети информации с помощью проходных сетевых шифраторов «КРИПТОН AncNet», обеспечивающих гарантированную защиту данных.

Архитектура защищенного «тонкого клиента» основана на использовании сертифицированных отечественных решений.

ЛИНЕЙКА ДОВЕРЕННЫХ КОМПЬЮТЕРОВ ОТЕЧЕСТВЕННОГО ПРОИЗВОДСТВА

Фирма «АНКАД» представляет также семейство доверенных компьютеров, разработанных в кооперации с отечественными технологическими партнерами.

Данное семейство основано на отечественной аппаратной платформе в виде линейки материнских плат с интегрированными средствами защиты, включая неизвлекаемый АПМДЗ «КРИПТОН-ВИТЯЗЬ», размещаемый непосредственно на материнской плате. Это позволяет поднять качество защиты на новый уровень, поскольку такая интеграция АПМДЗ дает возможность расширить область доверия на материнскую плату в целом и формировать на ее основе контуры защиты всей компьютерной системы.

Линейка доверенных компьютеров включает в себя сервер начального уровня, терминальные и рабочие станции и планшетные компьютеры. Все они имеют ряд отличительных особенностей, основными из которых являются следующие:

- доверенная аппаратная платформа российского производства с интегрированными функциями безопасности;
- универсальная доверенная среда на уровне UEFI для запуска модулей безопасности (включая антивирусную защиту);
- аппаратный контроль системных шин, гарантирующий неизменность BIOS компьютера;
- двухфакторная аутентификация;
- защищенное хранилище ключевой информации;
- доверенная загрузка операционной системы и контроль целостности программных компонентов.

* * *

В качестве заключения отмечу, что компетенция специалистов Фирмы «АНКАД» позволяет выполнять работы самого широкого профиля: от разработки элементной базы — до создания комплексных решений.

Мы готовы как выполнять доводку существующих систем защиты под специфические требования клиента, так и разрабатывать принципиально новые средства и решения по обеспечению информационной безопасности.