

Комплексные решения по защите государственной тайны

Юрий РОМАНЕЦ

Фирма «АНКАД» – ведущий российский разработчик и поставщик систем защиты информации в январе 2016 г. отмечает 25-летний юбилей.

Основу деятельности компании составляет разработка, производство и внедрение аппаратных средств криптографической защиты информации, средств защиты от несанкционированного доступа и комплексных решений по обеспечению информационной безопасности. Это инновационные продукты, защищенные российскими патентами, созданные на основе отечественных криптоалгоритмов и соответствующие самым высоким требованиям стандартов и системы сертификации ФСБ и ФСТЭК России.

Приоритетным для нас направлением является защита информации, составляющей государственную тайну, с высокими грифами секретности. Нам доверяют защиту своих информационных систем, в основном, крупные государственные и коммерческие организации, министерства, силовые ведомства – те, кому необходима надежная защита информации.

Одним из комплексных технических решений, на которые можно опираться при создании информационных систем, обрабатывающих критически важную информацию, является разработанная нами архитектура защищенного «тонкого клиента» «КРИПТОН-ТК».

Существуют определенные преимущества использования «тонкого клиента» применительно к компьютерным системам,



Юрий Васильевич РОМАНЕЦ – генеральный директор ООО Фирма «АНКАД»

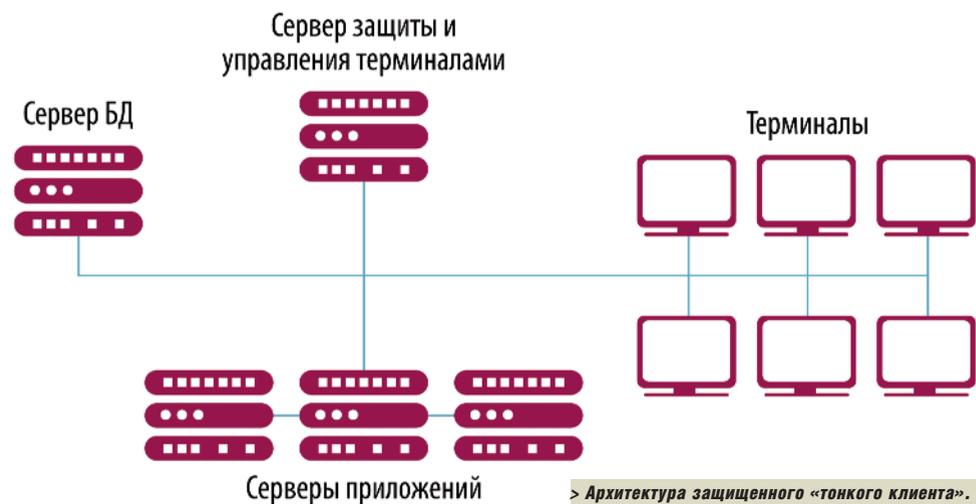
обрабатывающим информацию, содержащую государственную тайну, в частности:

- вся информация физически хранится и обрабатывается только на серверах, которые можно защитить организационными мерами;
- отсутствует информация на терминалах пользователей в выключенном состоянии;
- легкая адаптация архитектуры для использования в географически распределенных средах;

- возможность жесткого контроля информационных потоков в системе;
- централизованное администрирование и обновление системы;
- возможность организации полного мониторинга действий пользователей и управления системой в режиме реального времени.

Архитектура защищенного «тонкого клиента» позволяет обеспечить дальнейшее поэтапное усиление степени защиты информационных систем, в т. ч. 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. Единая многофакторная аутентификация и идентификация пользователя.
3. Централизованное защищенное хранение информации о субъектах и объектах системы, правил разграничения доступа и прочих настроек системы и ее отдельных компонентов позволяет гибко управлять правами доступа и параметрами пользователей, а также мгновенно распространять изменения на всю систему.



Архитектура защищенного «тонкого клиента».

Вся указанная информация может храниться на выделенном сервере баз данных с организацией доступа к ней только через сервер защиты и управления терминалами, осуществляющий авторизацию всех запросов к данным.

4. Доверенная загрузка рабочей операционной системы терминала (в качестве которой используется сертифицированная отечественная ОС) с сервера в среде АПМДЗ только после успешной аутентификации пользователя.

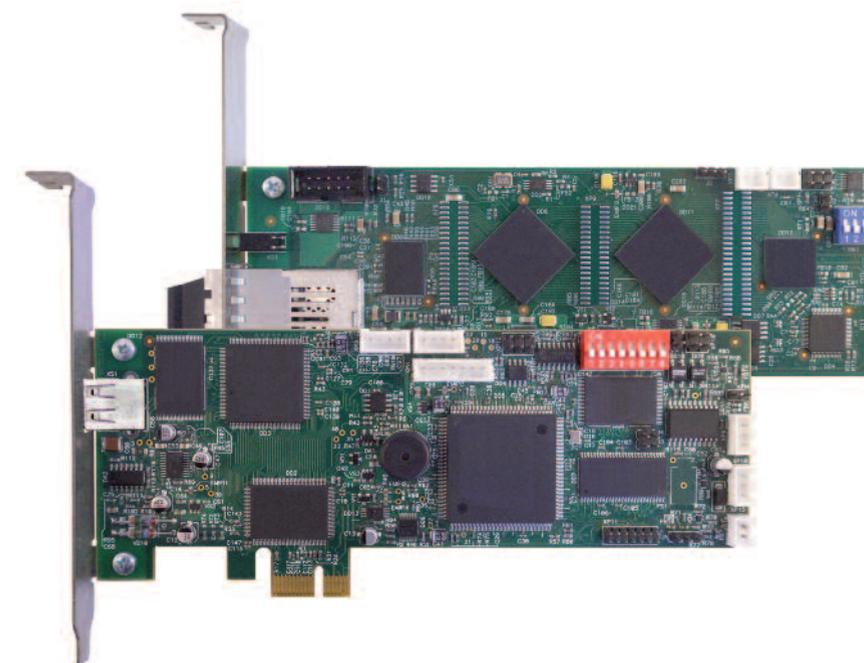
Поскольку ОС загружается в оперативную память терминала, она уничтожается после выключения питания терминала. Это позволяет избежать угрозы модификации или несанкционированного доступа к терминальной ОС.

5. Обеспечение разграничения доступа к объектам файловой системы серверов с помощью системы разграничения доступа «КРИПТОН-ЩИТ».

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

Отдельно стоит сказать про терминальное оборудование.

Наши терминалы основаны на использовании отечественных сертифицированных по требованиям ФСБ решений. В частности, терминал «КРИПТОН-ТК-ИК» выполнен на базе отечественной сертифицированной материнской платы KWBS со средствами защиты, интегрированными в нее на аппаратном уровне. На основе KWBS в настоящий момент разрабатывается базовое семейство средств вычислительной техники для МО РФ, включающее сервер начального уровня, настольный компьютер, ноутбук и планшет. Их использование позволяет значительно снизить зависимость от импортных СВТ в специальных вычислительных инфраструктурах, в т. ч. в ИС органов военного и государственного управления.



АПМДЗ «КРИПТОН-ЗАМОК» и проходной сетевой шифратор «КРИПТОН AncNet».



Пример защищенного терминала.

Существует также исполнение защищенного терминала с интегрированными средствами защиты в форм-факторе моноблока. В силу особенностей и характеристик, обеспечивающих чрезвычайно малые зоны побочных электромагнитных излучений, данный защищенный терминал может использоваться для специальных применений не только на территории РФ, но и за ее пределами.

Таким образом, архитектура защищенного «тонкого клиента» «КРИПТОН-ТК» имеет множество преимуществ в части обеспечения информационной безопасности по сравнению с классическими архитектурами построения распределенных компьютерных систем и, следовательно, может быть использована в

качестве основы для создания ИС, предназначенных для обработки критически важной информации.

В качестве заключения отмечу, что Фирма «АНКАД» имеет многолетний опыт работ по обеспечению информационной безопасности по самым высоким уровням требований. Наша компания открыта для сотрудничества с организациями, разделяющими

нашу главную цель: обеспечение информационной безопасности России для укрепления обороноспособности страны.



ООО Фирма «АНКАД»
124498, г. Москва, г. Зеленоград,
проезд 4806, дом 5, строение 20
Тел.: (499) 731-0000, 732-1313
E-mail : marketing@ancud.ru
www.ancud.ru