БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Бородич С.В.* ЭМС наземных и космических радиослужб. – Москва: Радио и связь, 1990.
2. *Круглов В.В., Борисов В.В., Харитонов Е.В.* Нейронные сети: конфигурации, обучение, применение. – Смоленск: Изд-во Моск. энерг. ин-та, филиал в г.Смоленске, 1998.
3. *Muller B., Reinhardt J.* Neural Networks. An introduction. – Berlin: Springer-Verlag, 1991.
4. *Тепляков И.М., Калашников И.Д., Рощин Б.В.* Радиолинии космических систем передачи информации. – Москва: Советское радио, 1975.

УДК 681.53

Е.Ф. Стукалина, Н.С. Марков, К.С. Масленников

СПЕЦИФИКА ВНЕДРЕНИЯ ТЕХНОЛОГИИ PKI

Внедрение PKI представляет собой сложный и трудоемкий процесс. От его правильной организации, в конечном итоге, зависит эффективность функционирования инфраструктуры безопасности информационной системы, равно как и самой информационной системы в целом.

PKI-решение, как правило, внедряется в уже существующую IT-инфраструктуру с определенными механизмами взаимодействия компонент.

Специфика предлагаемого проекта внедрения технологии PKI заключается в модернизации уже существующей доменной архитектуры рассматриваемого подразделения Ижевского государственного технического университета – кафедры «Системы и технологии информационной безопасности».

Действующий вариант построения сети и доверительных отношений между ее хостами затрудняет полный переход на новый организационный уровень. Причиной являются следующие факторы:

- внедрение технологии «активной директории» (Active Directory) на существующую доменную структуру возможно; следует учесть, что при этом будет не полностью реализована политика безопасности контроллера домена (Domain Security Policy) требуемого уровня, так как последовательность построения новой системы в целом нарушена; это во многом определяет корректность работы служб центра сертификации;
- ряд сетевого программного обеспечения, функционирующего в уже существующей иерархии и использующего жесткую регламентацию разделения прав доступа пользователей к предоставленным ресурсам (например, Microsoft Internet Information Security), может перестать корректно выполнять возложенные функции в связи с реорганизацией системы распределения доступа учетным записям к сетевым и локальным ресурсам и изменением политики безопасности, как контроллера домена, так и самого выделенного сервера.

Для более детальной отработки процедуры миграции на принципиально новый уровень иерархии построения сети и доверительных отношений между хостами предложен вариант введения в опытную эксплуатацию проекта, используя программное обеспечение VMware Workstation 6.0.2 (Build 59824), позволяющее строить модели виртуальных машин и сетей. Данное решение позволит детально проанализировать процесс миграции, определить минимальные требования для реализации наиболее полного решения перехода к технологии PKI.

На сегодняшний день стоит учитыватьть тот факт, что опытная эксплуатация во многом будет предопределена в основном учебным процессом и лишь отчасти будет обеспечивать информационную безопасность кафедры «Системы и технологии информационной безопасности». Для обеспечения полнофункцио-

нальной политики информационной безопасности на основе иерархии PKI необходимо внедрение технологии на уровне всего учебного учреждения. Распространение технологии, по крайней мере первое время, будет достаточно ограниченным. Наиболее приемлемым вариантом будет отказаться от передовых промышленных продуктов, таких как Baltimore и Entrust, и реализовать иерархию, используя исключительно средства сетевой операционной системы Microsoft Windows 2003 Server Enterprise Edition.

Стоит учесть и аргумент в пользу выбранного продукта – рассматриваемая нами операционная система реализует наиболее передовые технологии PKI, такие как autoenrollment, которых нет в продуктах Baltimore и Entrust.

Третья версия технологии Microsoft PKI более масштабируема, более гибкая в использовании и настройке, позволяет достаточно просто наращивать структуру. Вот отличие от относительно устаревших серверных вариантов операционных систем (они встречаются и в настоящее время) Windows 2000 Server и Windows NT был сделан значительный шаг в развитии технологии:

- *масштабируемость.* Windows Server 2003 PKI имеет практически неограниченные возможности в расширении структурной схемы при условии, что речь идет о ряде центров сертификации (ЦС или CA). Высокий уровень масштабируемости достигается тем, что, начиная с Microsoft Windows 2000 Server, использованы технологии JET Blue для построения, поддержания работоспособности базы данных CA. Наиболее важным фактом является поддержка многоуровневой иерархии ЦС, состоящая из корневого ЦС и нескольких уровней (до 40) подчиненных ЦС. Операционная система Windows NT 4 поддерживает только два уровня иерархии;
- *гибкость.* Windows Server 2003 CA может быть установленным в двух режимах: enterprise или stand-alone. Каждый из режимов строится с учетом уровня потребностей конкретного предприятия в области безопасности. Одна из наиболее важных особенностей Windows Server 2003 PKI, состоит в том, что администратор имеет полный контроль за содержимым сертификата Windows Server 2003 certificate (осуществляется с помощью редактируемых шаблонов сертификатов);
- *совместимость.* Microsoft PKI поддерживает основные открытые стандарты: ITU-T X.509, IETF PKIX, PKCS. Windows Server 2003 PKI поддерживает широкий спектр криптографических алгоритмов: RSA, DSA, RC4, AES, и так далее. В операционной системе Windows Server 2003 CA могут быть использованы PKI программного обеспечения от других производителей;
- *расширяемость*. Сервис Windows Server 2003 CA является расширяемым. Его политика безопасности и выходные модули могут быть настроены конкретно с учетом требований определенной организационной структуры. Для удовлетворения современных требований безопасности Windows Server 2003 CA поддерживает аппаратные модули защиты информации (HSM). В том числе существует интеграция технологии PKI в приложения, тем самым обеспечивая должным уровнем информационную безопасность внутри сети (хорошим примером является поддержка CAPICOM).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Microsoft Corporation. Microsoft Windows Server TechCenter. http://technet2.microsoft.com/windowsserver/en/technologies/featured/gensec/ /default.mspx (21 мар. 2008).
2. *Минаева Е.В., Любко А.А.* Программирование приложений инфраструктуры открытых ключей на платформе Microsoft .NET (2004). Учебный Центр безопасности информационных технологий Microsoft Московского инженерно-физического института.
3. http://devgroup.mephist.ru/pkinet.aspx (18 фев. 2008).