

Вторая Всероссийская конференция
«Информационные технологии в России»

СЕКЦИЯ

**СИСТЕМЫ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**

Тезисы докладов

26 - 28 сентября 2001 г.
Москва, ВВЦ (ВДНХ), павильон № 69

**Вторая Всероссийская конференция
«Информационные технологии в России»**

**Секция:
«Системы информационной безопасности»**

РАСПИСАНИЕ

Место проведения – Москва, ВВЦ (ВДНХ), павильон № 69
26 - 28 сентября 2001 г.

26 сентября	10:00 – 18:00	Информационная безопасность для корпоративных пользователей. Решения для MS Windows 2000.	Большой конференц- зал
27 сентября	10:00 – 13:00 14:00 – 18:00	Решения по информационной безопасности для корпоративных пользователей. Секция для производителей систем информационной безопасности.	Аудитория 201
28 сентября	10:00 – 18:00	Информационная безопасность для корпоративных пользователей. Решения по безопасности для Novell NetWare. Презентация Novell NetWare 6.0.	Деловой центр

Организаторы:

- Компания "ИТ-экспо"
- Издательство "Открытые системы"
- Компания Aladdin Software Security R.D.

Учредители:

- Министерство промышленности, науки и технологий РФ
- Российская Академия Наук
- Правительство Москвы

Спонсоры:

- Microsoft
- Novell
- Aladdin Software Security R.D.
- ALERO Software Alliance B.V.

26 сентября 2001 г.

БОЛЬШОЙ КОНФЕРЕНЦ-ЗАЛ

Подсекция:

Информационная безопасность для корпоративных пользователей.

Решения для MS Windows 2000

Ведущий:

Дмитрий Вишняков, Московское Представительство Microsoft

РАСПИСАНИЕ

- 10:00** Открытие конференции по информационной безопасности. *А. Каландин, Гостехкомиссия России*
- 10:15** Законодательство РФ и криптография. Политика ФАПСИ в области распространения и использования криптосредств. *Д. Ульянов, В. Мартынов, ФАПСИ*
- 10:40** Развитие рынка систем информационной безопасности. *С. Груздев, Aladdin Software Security R.D.*
- 11:05** Концепция обеспечения безопасности в Windows 2000. *Д. Вишняков, Microsoft*
- 12:15** Средства криптографической защиты в ОС Windows. *И. Курепкин, Крипто-Про*
- 12:40** Индустриальный стандарт PKI. Обзор различных систем PKI, представленных на российском рынке. Методика построения PKI. *Д. Шепелявый, Информзащита*
- 13:25** Токены в системах информационной безопасности. Обзор мирового рынка. *Y. Margalit, Aladdin Knowledge Systems*
- 13:50** Российская интеллектуальная карта (РИК). Возможности и перспективы применения. *А. Бубеничек, НТЦ «АТЛАС»*
- 14:15** USB-брелок eToken как важный элемент систем информационной безопасности. *С. Груздев, Aladdin Software Security R.D.*
- 14:40** Безопасность в платежных системах на базе микропроцессорных пластиковых карт. *В. Евтушенко, BGS*
- 15:05** eToken - ключ XXI века для удобной и безопасной работы в сети Windows 2000/XP. *А. Крючков, Quarta Technologies*
- 15:30** Защищенные виртуальные частные сети. Рынок средств построения VPN и соответствующие решения. *А. Соколов, ЭЛВИС+*
- 16:00** Обеспечение Информационной безопасности в решениях для Lotus Notes. *А. Савельев, ИнтерТраст*
- 16:25** Организация защищенного доступа к информационным ресурсам предприятия через глобальные сети (демонстрация). *В. Зинченко, ВПП-Телеком*
- 16:50** Защищенная почтовая система как основа информационной безопасности предприятия («The Bat! Pro»). *С. Демченко, RitLabs*
- 17:15** Защищенный доступ удаленных клиентов к корпоративной сети. Check Point Next Generation. *Н. Фомиченко, Корпорация ЮНИ*

27 сентября 2001 г.

АУДИТОРИЯ №201

Подсекция:

Решения по информационной безопасности для корпоративных пользователей.

Секция для производителей систем информационной безопасности

Ведущий:

Сергей Александров, Aladdin Software Security R.D.

РАСПИСАНИЕ

- 10:00** Открытие второго дня конференции. *С.Александров, Aladdin Software Security R.D.*
- 10:10** Цифровая подпись: технология настоящая и ее имитации. Отраслевые и корпоративные стандарты цифровой аутентификации. *А. Лебедев, ЛАН Крипто*
- 10:35** Усиленная аутентификация пользователей при доступе к системе управления предприятием SAP R/3. *А. Садердинов, Мекомп*
- 10:50** Усиленная аутентификация пользователей в системе «1С:Предприятие». Система O'Key 7.7. *Е. Виноградова, 1-й Архитектор бизнеса*
- 11:15** Усиленная аутентификация пользователей в системе управления документами Documentum 4i. *К. Синюшин, Documentum*
- 11:40** Усиленная аутентификация пользователей в системах управления документами DOCS Open и CyberDOCS. *М. Ферапонтов, Весть-МетаТехнология*
- 12:05** Обеспечение безопасности корпоративных информационных порталов. *С. Артемов, Город-Инфо*
- 12:30** Усиленная аутентификация удаленных клиентов в терминальных решениях (на примере Citrix Metaframe). *С. Калачев, Expert Mark*
- Перерыв (13-00 - 14-00)**
- 14:05** Партнерская программа компании Aladdin. Сертификация решений и их продвижение на мировой рынок. Планы компании. *Y. Margalit, Aladdin Knowledge Systems*
- 14:30** ALERO - издание и продвижение русских продуктов за рубежом. *S. Desourdy, ALERO Software Alliance B.V.*
- 14:55** Организация распространения программного обеспечения через Интернет по схеме Try-Before-You-Buy. Дистанционное перепрограммирование eToken. *С. Груздев, А. Раевский, Aladdin Software Security R.D.*
- 15:20** Инфраструктура продажи ПО через Интернет. Служба регистрации Shareware. *Ф. Мучник, «ТФМ и К»*
- 15:50** Сервис-дистрибуция решений по информационной безопасности. Проект InfoSecurity.ru. *Ф. Ушаков, Служба F1*
- 16:15** eToken Internet Logon - безопасный доступ в Интернет с защитой паролей от кражи. *Ю. Илларионов, Infotex*
- 16:40** Secret Disk - система защиты конфиденциальной информации. *А. Куприянов, Aladdin Software Security R.D.*
- 17:05** Преступления в сфере компьютерной информации. Опыт борьбы на примере Перми и Пермской области. *О. Искандаров, «Управление Р» Пермского ГУВД*

28 сентября 2001 г.

ДЕЛОВОЙ ЦЕНТР

Подсекция:

Информационная безопасность для корпоративных пользователей.

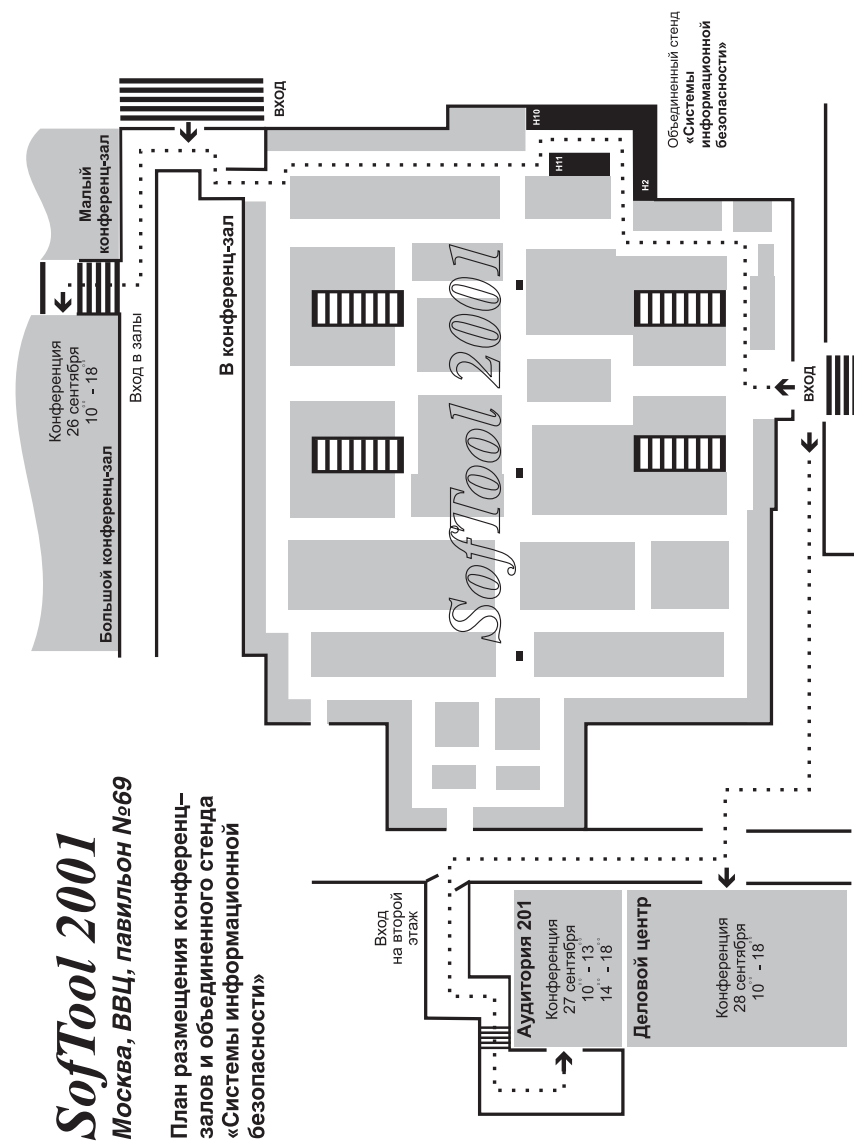
Решения для Novell NetWare

Ведущий:

Михаил Елашкин, Московское представительство Novell

РАСПИСАНИЕ

- 10:00** Открытие третьего дня конференции. *М. Елашкин, NOVELL*
- 10:10** Управление безопасностью в корпоративных информационных системах: eSafe - комплексная технология защиты информации. *И. Ляпунов, ЛАНИТ*
- 10:35** Информационная безопасность и современная криптография: методы, проблемы, регулирование. *А. Лебедев, ЛАН Кристо*
- 11:00** Защита от искажения и подделки информации в Интернете. Цифровые сертификаты Thawte. *А. Глазков, РосБизнесКонсалтинг*
- 11:25** Особенности современных PKI-систем. RSA Keon Advanced PKI. *Р. Кашанов, Demos*
- 11:50** Инфраструктура открытых ключей на основе Baltimore UniCERT. *С. Знаменский, Hewlett-Packard*
- 12:15** Защищенный клиент Check Point SecuRemote VPN-1. Сертифицированное OPSEC решение. *И. Кораблев, Безопасные Информационные Технологии*
- 12:40** Безопасное подключение локальных сетей к открытым ресурсам Интернет на базе технологий VPN. *В. Игнатов, ИнфоТеКС*
- 13:05** Технологии защиты от несанкционированного доступа в клиент-серверных приложениях. Система Matrix. *М. Кириллов, ЛАНИТ*
- 13:30** Семейство межсетевых экранов и VPN-построителей ФПСУ-IP с усиленной аутентификацией пользователей. *М. Беребень, АМИКОН*
- 14:00** Презентация Novell NetWare 6.0. *М. Елашкин, А. Жерлицын, К. Степанов, Novell*
- 16:20** Серверные решения Compaq. *М. Криворученко, Compaq*
- 17:00** Secret Disk Server - система «прозрачного» шифрования томов NetWare с возможностью мгновенного отключения. Защищенный Backup. *А. Бевз, Aladdin Software Security R.D.*
- 17:15** Усиление серверных процедур идентификации и аутентификации NDS eDirectory и BorderManager и контроль их целостности. Защищенные клиенты Trusted Login. *Г. Лебедев, А. Шакунов, БИТС*
- 17:40** Многоуровневая среда управления безопасностью корпоративных систем в гетерогенных сетях. *А. Шакунов, БИТС*



Законодательство РФ и криптография. Политика ФАПСИ в области распространения и использования криптосредств

Д.Ульянов, заместитель начальника отдела, Н. Мурашев, ведущий инженер, Отдел Лицензионного и сертификационного центра ФАПСИ

1. Законодательное регулирование работ и услуг, связанных с криптографией, как частный случай лицензирования отдельных видов деятельности. Критерии определения лицензируемых видов деятельности.
2. Обзор нормативной правовой базы Российской Федерации, регламентирующей деятельность в области защиты информации, с 1994 года по настоящее время. Тенденции ее развития.
3. Политика ФАПСИ в отношении оборота российских СКЗИ – поддержка легитимного разработчика.
4. Политика ФАПСИ в отношении оборота иностранных СКЗИ – стремление к оптимальному сочетанию поддержки отечественного производителя и учета международных реалий.
5. Политика ФАПСИ в области использования коммерческих СКЗИ – субъекты регулирования, лицензионная и регистрационная системы.

Развитие рынка систем информационной безопасности

С. Груздев, генеральный директор, Aladdin Software Security R.D.

Рынок систем информационной безопасности (СИБ) – наиболее быстрорастущий и востребованный на сегодняшний день. Согласно данным IDC, рынок ПО информационной безопасности почти утроится к 2005 году. Доходы на нем повысятся с \$5,1 млрд. (прошлогодний результат) до \$14 млрд.

Сегменты рынка СИБ, развивающиеся наиболее активно:

- антивирусы;
- firewalls;
- VPN;
- PKI;
- AAA (аутентификация, авторизация, администрирование) – наиболее быстро развивающийся. По прогнозам аналитиков, будет расти на 28% ежегодно до \$9,5 млрд. в 2005 году.

В настоящее время четко прослеживаются две тенденции: тяготение бизнеса к Интернету и повсеместное (как в масштабах предприятия, так и в масштабах страны и мира) использование PKI. Они вызывают рост рынка систем аутентификации.

Одна из основных проблем этого сегмента – поиск защищенного хранилища для аутентификационной информации (цифровых сертификатов, ЭЦП и т.д.) Оно должно обладать тремя основными качествами: компактностью, защищенностью и удобством в применении. Этим требованиям отвечают токены, обладающие в то же время полной функциональностью смарт-карт и следующими преимуществами:

- аутентификация как пользователя, так и приложения;
- двухфакторная (программно-аппаратная) аутентификация;
- аппаратная реализация криптоалгоритмов.

Наиболее платежеспособным и ресурсоемким рынком систем информационной безопасности сейчас является рынок США, однако один из самых динамичных – рынок России. Интенсивность его роста в России достигает 100% в год. Именно российские разработки в области информационной безопасности находятся сейчас в фокусе внимания западных компаний, а наиболее качественные продукты с успехом продаются на западных рынках. Однако, несмотря на высокий экспортный потенциал, в силу ряда причин заниматься легальным экспортом российским компаниям трудно; подчас это даже убыточно. С помощью образующегося Альянса компаний-участников рынка информационной безопасности эта проблема должна быть решена. Главная же цель Альянса – построение цивилизованного рынка в России.

Концепция обеспечения безопасности в Microsoft Windows 2000

Дмитрий Вишняков, системный инженер, Microsoft

Система безопасности операционной системы Microsoft Windows 2000 решает следующие ключевые задачи: аутентификация пользователей, авторизация доступа пользователей к ресурсам, обеспечение конфиденциальности и целостности данных, хранящихся на носителях и передаваемых по сети.

Проверку однозначного соответствия пользователя и субъекта системы безопасности осуществляют службы аутентификации. Процесс аутентификации начинается с того, что пользователь сообщает системе свои регистрационные параметры, как правило – регистрационное имя и пароль. Службы аутентификации проверяют соответствие введенных данных параметрам, хранящимся в базе данных. При успешной проверке создается сеанс пользователя, а для субъекта формируется маркер доступа. Windows 2000 поддерживает несколько протоколов аутентификации, при этом основным протоколом является Kerberos версии 5. Средствами Windows 2000 Server можно развернуть полноценную инфраструктуру открытых ключей и организовать аутентификацию пользователей с помощью смарткарт.

Функции контроля доступа системы безопасности Windows 2000 позволяют назначать и контролировать права доступа пользователей к защищаемым объектам, а также ограничивать административные привилегии, предоставляемые пользователям для выполнения тех или иных действий.

Доступ к службам криптографии Windows 2000 организован посредством прикладных программных интерфейсов CryptoAPI: для выполнения какой-либо криптографической операции приложение должно явно обратиться к методам CryptoAPI. Криптографические службы, включая защищенное хранилище криптографических ключей, реализованы в рамках независимых модулей – Cryptographic Service Providers (CSPs).

Windows 2000 Server включает в себя набор служб, технологий, протоколов и стандартов, позволяющих организовать систему защиты информации на базе шифрования с использованием пар ключей: открытый(публичный)/закрытый (личный). Инфраструктура открытых ключей Windows 2000 базируется на Центре сертификации Microsoft и реализует стандарты PKIX X.509.

Файлы, хранящиеся на жестком диске компьютера, защищены от несанкционированного доступа с помощью механизмов контроля доступа. Тем не менее, возможны ситуации, когда субъект получает доступ к файлу в обход системы безопасности. Конфиденциальность данных, расположенных на жестком диске компьютера, обеспечивает служба Encrypting File System (EFS). Сфера действия этой службы заканчивается, как только файл покидает том NTFS: данные, зашифрованные EFS, передаются в локальную сеть в расшифрованном виде. Следовательно, для сохранения конфиденциальности данных необходимы механизмы защиты сетевого потока.

На высоком уровне – на уровне приложений – можно использовать протокол защиты сетевых данных SSL, но для этого необходимо, чтобы само приложение, посылающее данные в сеть (или получающее их из сети), поддерживало протокол SSL, т.е. могло явно обращаться к соответствующим интерфейсам. Чтобы избавить приложения от необходимости самостоятельно заботиться о защите передаваемой информации, нужны механизмы, работающие на более низком уровне – на уровне сети. Такие механизмы реализованы в виде Протокола IP Security (IPSec), разработанного IETF.

Средства криптографической защиты в ОС Windows

И. Курепкин, руководитель отдела внедрения, Крипто-Про

Доклад приводит описание архитектуры криптографических функций, разработанной корпорацией Microsoft для операционных систем Windows, способы использования криптографических функций в различных прикладных системах Microsoft и пользовательском прикладном обеспечении. В докладе приводится описание средства криптографической защиты информации КриптоПро CSP, разработанного в соответствии с интерфейсами Microsoft.

- Архитектура криптографических функций в операционных системах MS Windows
- Назначение интерфейса CryptoAPI
- Описание интерфейса CryptoAPI
 - Функции работы со справочниками
 - Функция обработки криптографических сообщений
 - Функции кодирования/декодирования объектов
 - Базовые криптографические функции
- Интерфейс Cryptographic Service Provider (CSP)
- Средство криптографической защиты информации КриптоПро CSP
- Основные характеристики КриптоПро CSP
- Ключевые носители
- Инфраструктура открытых ключей
- Использование КриптоПро CSP
 - Защищенная почта (S/MIME)
 - Контроль распространяемого программного обеспечения
 - Встраивание в приложения
 - Службы сертификации открытых ключей
 - Защита соединений в сети Интернет
- КриптоПро TLS

Индустриальный стандарт PKI. Обзор различных систем PKI, представленных на российском рынке. Методика построения PKI

Д. Шепелявый, заместитель директора по консалтингу, Информзащита

В докладе рассматриваются критерии оценки решений PKI, предлагаемых для построения инфраструктуры управления информационной безопасностью корпоративных систем, а также излагается методика построения PKI.

Принятие решения о применении PKI имеет серьезное значение для компании. Технология PKI является одним из немногих решений в области информационной безопасности, напрямую затрагивающих бизнес-процессы предприятия. Поэтому от грамотности и обоснованности выбора решения для построения PKI будет зависеть не только эффективность вложений в IT, но и эффективность бизнеса в целом.

Решения PKI можно оценивать по следующим критериям:

- поддерживаемые форматы сертификатов;
- методы генерации и отзыва сертификатов;
- масштабируемость и модульность системы PKI;
- безопасность и удобство администрирования системы управления PKI;
- поддерживаемые топологии инфраструктуры открытых ключей;
- удобство администрирования PKI;
- поддержка открытых стандартов;
- дополнительные возможности.

Используя критерии, описанные выше, было произведено краткое сравнение параметров основных систем PKI, предлагаемых на российском рынке, а именно Baltimore Unicert v3.51, RSA Keon 5.0 и реализация PKI в MS Windows 2000.

Работы по сравнению решений PKI на самом деле являются составной частью комплексной методики построения PKI, которая состоит из следующих шагов:

- анализ бизнес-требований (**Requirements Analysis**);
- выработка архитектуры PKI (**Definition**);
- описание функционирования PKI (**Operations**);
- оценка рисков (**Security Review**);
- интеграция компонент PKI (**Integration**);
- внедрение PKI (**Deployment**);
- сопровождение PKI (**Post-Deployment**).

Очевидно, что построение PKI требует ясного осознания требований к инфраструктуре открытых ключей, а также четкого проектирования и грамотного внедрения. Только тогда инвестиции в PKI окажутся выгодными, а польза – ощутимой.

eToken как элемент системы информационной безопасности

С. Груздев, генеральный директор, Aladdin Software Security R.D.

I. Любой продукт в области информационной безопасности предполагает две компоненты:

- аутентификация пользователя (проверка права обращаться и работать с данной информацией). Программная (парольная) защита уже не оправдывает себя; более надежные и предпочтительные средства – аппаратные;
- обеспечение надежного хранения ключей и сертификатов.

II. Ранее в качестве носителей идентификационной информации использовались дискеты, затем – таблетки touch memory; решения на базе смарткарт. Однако на рынке этих средств образовался вакуум в ценовом диапазоне от \$20 до \$50. Его заполнил новый класс устройств с аналогичными по отношению к смарткарт-технологиям функциями – токены.

III. Три года назад прогнозировалось резкое падение цен на считывающие устройства и снабжение ими к 2000 г. 90-95% компьютеров; этого не произошло, в частности, по следующим причинам:

- высокая цена считывающих устройств;
- ценность портов, к которым они подключаются, как ресурса, необходимого также и для других устройств. Кроме того, стандарт PC 99 не предполагает наличия последовательных и параллельных портов, к которым подключаются считывающие устройства и ридеры для touch memory.

IV. Токены: на стыке технологии USB и смарткарт-технологий. Представляют из себя USB-ключи форме брелка с полной функциональностью смарткарт. Функции:

- аутентификация при доступе к защищенным ресурсам;
- хранилище ключевой информации (цифровых сертификатов);
- подключение к различным информационным ресурсам, приложениям (вход в ОС Windows, в корпоративную сеть и т.д.)

Токен стал важнейшим элементом в системах информационной безопасности.

V. Компания Aladdin представляет три модели USB-ключей eToken:

- eToken R2 (с аппаратной реализацией несимметричной криптографии);
- eToken Pro (с аппаратной реализацией симметричной криптографии);
- eToken РИК (с аппаратной реализацией отечественного алгоритма ГОСТ 28147-89; содержит сертифицированный ФАПСи кристалл РИК).

eToken РИК имеет также функции диверсификации ключа и генерации сеансовых ключей. Кроме того, он обладает двойной функциональностью: может быть использован для проведения платежей через Интернет, поскольку обеспечивает безопасный обмен транзакциями, а также применяем в локальных платежных системах. С помощью eToken РИК решается основная задача – стопроцентная аутентификация пользователя – при проведении транзакции. В связи с этим eToken РИК представляет значительный интерес для зарубежных заказчиков и обладает высоким экспортным потенциалом.

Безопасность в платежных системах на базе микропроцессорных пластиковых карт

В. Евтушенко, начальник отдела BGS Smartcard Systems AG

1. Безопасность платежной системы как мера устойчивости системы ко внешним воздействиям, которые могут повлечь за собой финансовые потери.

Платежная система как финансовый инструмент организации безналичного оборота средств является в такой же степени интересным для взлома объектом, как, скажем, и сейф с наличными деньгами. С той только разницей, что масштабы потенциальных хищений, а, значит, и ежедневных рисков неизмеримо больше, а возможности у злоумышленника уйти от ответственности значительно богаче. Особенно актуальным этот тезис становится в современном мире электронной торговли и электронных денег. Таким образом, наиважнейшим критерием пригодности платежной системы к выполнению основной задачи – обеспечению взаиморасчетов – является устойчивость, т.е. возможность системы сохранять свои свойства в условиях возмущающих внешних воздействий.

2. Обеспечение безопасности – комплекс взаимосвязанных задач на всех этапах проектирования и жизни системы.

Абстрактно мера безопасности может быть представлена как функционал, отображающий пространство проектных и эксплуатационных характеристик системы в пространство ее свойств устойчивости к внешним воздействиям. В реальной жизни обеспечение безопасности представляет собой решение комплекса задач по наделению системы заранее заданными свойствами. Исходные данные здесь принято называть «анализом рисков» или «управлением рисками». Другим важным аспектом является сбалансированность и разумная достаточность мер защиты. Говоря финансовым языком, собственно защита не должна стоить дороже защищаемого объекта.

3. Криптографические методы защиты информации.

Так или иначе, обеспечение безопасности есть защита информации от нежелательного с т.з. правил системы разглашения или искажения. Единственным практическим средством надежно защитить информацию являются криптографические методы. В связи с этим краеугольным камнем любой надежной платежной системы является методика и подсистема генерации, распределения и использования ключевой информации на всех функциональных уровнях.

4. Требования к архитектуре безопасной платежной системы.

Безопасная платежная система должна иметь особую, на сегодня уже признанную де-факто стандартную, архитектуру. Основная идея состоит в построении иерархических структур, где соблюдается главный схемотехнический принцип – чем ниже уровень, тем меньше ответственности ему делегируется и тем больше мер обеспечения безопасности применяется. Говоря конкретно, микропроцессорная карта проходит путь от главного системообразующего центра доверия до конкретного лица, держателя карты.

5. Современные программные и аппаратные средства защиты информации в приложениях к платежным системам.

Разработчики платежных систем сегодня имеют исключительно широкий выбор стандартных программных и аппаратных средств защиты, начиная от собственно микропроцессорных карт и заканчивая операционными системами и СУБД, включающими компоненты безопасности. Правильный выбор во многом определяет качество обеспечения безопасности. Решения компании Aladdin отличает нацеленность на нужды конкретного потребителя, высокое качество SDK, квалифицированная техническая поддержка. Появление нового поколения аппаратных средств защиты – eToken – предоставляет разработчикам и конечным пользователям совершенно новые возможности, а интеграция с изделиями РИК – ясную перспективу сертификации готовых решений согласно российским законам.

eToken – ключ XXI века для удобной и безопасной работы в сети Windows 2000/XP

А. Крючков, Quarta Technologies

Внедрение продукта позволит отказаться от использования паролей при входе в сеть и при защите конфиденциальной переписки. Пользователям не надо запоминать сложные пароли и периодически их менять – достаточно подключить электронный брелок eToken к USB-порту и ввести PIN-код. При этом значительно повышается защищенность сети и удобство работы. Возможности:

1. Аппаратная двухфакторная аутентификация пользователя при входе в сеть с помощью электронного USB-брелка eToken (Smart Card Network Logon). Использование усиленной аутентификации решает проблему подбора и перехвата паролей, что особенно актуально при удаленной работе в сети.
2. Блокирование компьютера (Lock) в перерывах между работой при отсоединении брелка eToken [опционально].
3. Автоматическое отключение от сети (Logoff) при отсоединении брелка eToken [опционально].
4. Хранение цифровых сертификатов X.509 в защищенной памяти брелка eToken, а не на диске.
5. PIN-авторизация пользователя при работе с брелком eToken. В целях безопасности пользователи могут периодически менять PIN-код для своего брелка eToken. Если eToken был потерян или украден, то никто, кроме хозяина, воспользоваться им не сможет: доступ к памяти защищен PIN-кодом.
6. Для защиты eToken используется аппаратная задержка отклика ~ 1 сек. Поэтому eToken никогда не блокируется.
7. Полная интеграция в Windows 2000/XP, поддержка PKI.
8. Возможность использования одного eToken различными приложениями, поддерживающими MS CryptoAPI 2.0.
9. Защита переписки для MS Outlook/Express (безопасное хранение сертификатов, защита от несанкционированного доступа, шифрование и цифровая подпись).
10. Возможность использования российских криптографических алгоритмов с длиной ключа 256 бит (сертифицированное ФАПСИ средство криптографической защиты информации КриптоПро CSP).
11. Генерация ключей производится пользователем самостоятельно.
12. Персонализация брелков eToken позволяет каждому брелку присвоить уникальное имя его владельца.

Защищенные виртуальные частные сети. Рынок средств построения SVPN и соответствующие решения

А. Соколов, генеральный директор, ЭЛВИС+

В последнее время все большее внимание уделяется технологии виртуальных частных сетей (VPN) как одному из базовых средств защиты информации, обрабатываемой в локальных и глобальных системах. Это обусловлено, в первую очередь, законным желанием собственника информации (будь то государство, организация или частное лицо) уберечь свою информацию от несанкционированного доступа при ее передаче по каналам связи.

Технология VPN позволяет превратить непредсказуемые связи открытых сетей (например, Интернета) в защищенные каналы, виртуально существующие в публичной сети. Эта возможность является чрезвычайно привлекательной, т.к. достигается значительная экономия финансовых средств за счет отказа от выделенных каналов связи. По мнению аналитиков, наиболее технологичным и экономичным способом сохранения вложенных в корпоративные информационные системы (КИС) инвестиций является создание VPN-системы на базе технологий, реализующих открытые и всесторонне проработанные интернет-стандарты. Важным моментом является и то, что VPN-система должна функционировать абсолютно прозрачно для уже существующих в КИС сервисов и приложений, а также быть полностью совместимой с используемыми в КИС сетевыми технологиями. По мере роста и развития КИС подсистема информационной безопасности (ПИБ) на базе VPN должна иметь возможность легко масштабироваться без потери целостности и управляемости.

Возрастание интереса пользователей к VPN подтверждается, например, ростом объемов продаж аппаратных и программных средств для формирования выделенных VPN до \$535 млн. во втором квартале 2001 г., что на 19% выше показателей первого квартала. На рынке сегодня имеются сотни предложений средств построения VPN, что затрудняет выбор пользователя. В докладе проводится анализ состава средств защиты информации, рассматриваются такие понятия, как VPN, SVPN, DPN, SVPN, ON, OSN, схемы построения различных типов защищенных сетей в зависимости от требований к сетевой инфраструктуре. Отмечается сдвиг внимания как разработчиков, так и пользователей в сторону повышения требований к средствам управления ресурсами безопасности, совместимости средств защиты различных производителей.

В заключение рассматривается новая версия продуктного ряда средств построения SVPN «ЗАСТАВА», удовлетворяющая на сегодняшний день на российском рынке запросам самого взыскательного пользователя. Продукты «ЗАСТАВА» обеспечивают конфиденциальность, аутентификацию и целостность информации в IP-сетях с помощью различных криптографических алгоритмов, подключаемых к VPN-продуктам через Open CryptoAPI интерфейс, что позволяет строить глобальные VPN-системы и, с учетом полной программной совместимости с продуктами Trustworks Security Suit компании Trustworks Systems, использовать криптографию по разные стороны национальных границ без технологических и правовых ограничений. Защита продуктами «ЗАСТАВА» прозрачна для всех сетевых сервисов и прикладных программ, не требует внесения изменений телекоммуникационной инфраструктуры и топологии сети. Решения на базе этих продуктов представляют широкий спектр возможностей: от защищенного диалога и канала связи между офисами до защищенной масштабной многоуровневой межкорпоративной инфраструктуры с системой PKI. Уникальный для российского рынка набор функциональных возможностей VPN «ЗАСТАВА» обеспечивает централизованное управление всей системой online, включая управление средствами защиты третьих производителей; поддержку режимов работы с мобильными клиентами; совместимость с системами, использующими Network Address Translation, с внешними PKI и токенами, а также с внешними системами сбора и обработки событий.

Обеспечение информационной безопасности в решениях для Lotus Notes

А. Савельев, директор по консалтингу, ИнтерТраст

1. Предметная область использования Lotus Notes

Возможности программного продукта Lotus Notes для построения корпоративной электронной почты и информационных систем документоориентированного характера. Прикладные задачи, решаемые в российских организациях на базе Lotus Notes. Услуги, предоставляемые ИнтерТраст по этому продукту и решениям на его основе.

2. Подключение к Lotus Notes внешних средств защиты информации

Почему встроенных средств защиты информации не хватает российским организациям? Что необходимо защищать, где и в какой момент времени должны выполняться криптографические операции над документами? «Locker» – решение от ИнтерТраст, обеспечивающее подключение внешних криптографических средств к Lotus Notes. Описание общих принципов работы, основные возможности. Варианты построения защищенных решений для Lotus Notes: для электронной почты (MailSecurity), для систем электронного документооборота, для других систем.

3. Усиленная аутентификация пользователей Lotus Notes с помощью eToken

«eToken для Lotus Notes» – решение от ИнтерТраст, позволяющее повысить безопасность работы в Lotus Notes за счет: обеспечения хранения в eToken ID-файла пользователя Lotus Notes; автоматического выполнения Login и Logout; автоматической установки сложных многозначковых паролей. Возможность использования одного eToken для хранения секретного ключа и ID-файла – объединение внешней криптографической защиты и защищенного входа в Lotus Notes.

Организация защищенного доступа к информационным ресурсам предприятия через глобальные сети (демонстрация)

В. Зинченко, директор департамента, VIP-Телеком

Основа успешной реализации сложного технического проекта – комплексный подход к проектированию системы с учетом всех выдвигаемых к системе технических требований.

В 1998 году компания VIP-Telecom, занимающаяся обслуживанием группы компаний «Vision International People Group», встала перед необходимостью разработки информационной системы, обеспечивающей защищенный доступ к оперативной информации с удаленных рабочих мест через неустойчивые каналы связи и сеть Интернет. Отказ от дорогостоящих выделенных каналов связи поставил разработчиков перед необходимостью выбора между технологией CORBA или технологией применения мониторов распределенных транзакций. В результате проведения экспертной оценки программных продуктов выбор пал на TUXEDO (BEA Systems).

Архитектура системы предполагает использование сети Интернет как транспортной среды для передачи данных, обрабатываемых в системе. Система построена по классической трехуровневой архитектуре и состоит из следующих компонентов:

1. Распределенная база данных на нескольких серверах MS SQL Server 7.0, функционирующих в локальной сети компании.
2. Сервер приложений на основе монитора транзакций BEA Tuxedo. В качестве составной части сервера приложений функционирует несколько процессов (задач), обеспечивающих функциональность запросов к серверам базы данных.
3. Комплект клиентских апплетов, покрывающий необходимый набор функций системы. Каждый клиентский апплет размещается на своей HTML-странице. Параметры соединения устанавливаются в тексте HTML-страницы и поэтому не требуют от конечного пользователя никаких дополнительных настроек.

Дополнительными преимуществами системы являются независимость от платформы (обеспечивается языком Java) и доступность (необходимо наличие только браузера, поддерживающего Java).

Аутентификация пользователя и определение уровня его доступа к данным обеспечивается применением ключей eToken компании Aladdin.

Обеспечивается высокая отказоустойчивость и надежность работы при работе на неустойчивых каналах связи.

Использование данного технического решения возможно при построении автоматизированных систем, к которым предъявляются повышенные требования к защите данных.

Защищенный доступ удаленных клиентов к корпоративной сети. Check Point Next Generation

Н. Фомиченко, Корпорация ЮНИ

1. Причины появления новой версии CheckPoint NG

Обеспечение безопасности становится все более сложной задачей, растет количество точек контроля, растет количество пользователей. Трафик через Интернет удваивается с каждым годом.

Требуется новый подход к средствам безопасности, обеспечивающий единую платформу управления с возможностью управления большим количеством удаленных сайтов.

2. VPN в Next Generation

Современные требования к Виртуальным Частным Сетям. Защита удаленных клиентов в Next Generation, интерфейс, средства централизованного управления для системного администратора. Новые возможности защиты удаленных клиентов. Отличия от предыдущей версии.

3. Защита компьютера удаленного клиента с помощью аппаратного ключа eToken

Проблема защиты компьютера удаленного клиента. Предложение OPSEC-партнера Checkpoint – компании Aladdin. Электронный ключ eToken добавляет новую функциональность для защиты удаленных клиентов корпоративной сети.

Усиленная аутентификация пользователей в системе «1С:Предприятие». Система O'Key 7.7

Е. Виноградова, руководитель отдела маркетинга, 1-й Архитектор бизнеса

Продукты системы «1С: Предприятие» занимают более 50% рынка делового ПО. Количество владельцев средств для авторизации доступа вырастает на 40% ежегодно. Популярность этих технологий объясняется оптимальным сочетанием удобства, простоты, надежности и цены. «O'KEY 7.7» встраивается в любую конфигурацию системы «1С: Предприятие», нетиповые в том числе, получила сертификат «Совместимо! Система программ 1С: Предприятие», продается через обе компании: «Аладдин» и «1С».

Работа с ключом eToken дает много новых возможностей пользователям системы «1С:Предприятие».

Личная идентификация

При входе в систему каждый сотрудник подключает персональный электронный ключ к шине USB для идентификации. Не надо запоминать пароли, а надежность системы возрастает.

Разграничение прав доступа

Если необходимо использовать не только систему идентификации, но и разграничение доступа к данным, то можно потребовать вводить для каждого электронного ключа персональный идентификационный номер (PIN).

Двойная авторизация

PIN-код служит и укреплению режима безопасности. Даже утеря ключа не создает опасности для сохранности данных.

Скрытое ограничение прав доступа

Особо ценные ресурсы информационной системы нуждаются в дополнительной защите. Невидимая, негласная для пользователя защита в компоненте «O'KEY 7.7» предохраняет от попыток взлома.

При обращении к защищенным данным система требует дополнительной идентификации. При неудачной идентификации пользователь получает доступ только к открытым данным или читает сообщение о системной ошибке.

Авторизация документов

На одном компьютере работает несколько пользователей (например, продавцы в торговом зале). Необходимо знать автора каждого созданного документа.

Достаточно установить ключ при проведении документа или формировании отчета.

Контроль персонала

Регистрация событий. Один из вариантов: работник, входящий в офис, использует ключ и вводит PIN-код для регистрации момента своего появления на работе и открывания двери. Так автоматизируется процесс заполнения табеля.

Вызов скрытых форм

Представьте себе – интерфейс без каких-либо пунктов доступа. Пользователь подключает ключ: на экране возникает форма с кнопками, заменяющая собой интерфейс.

Конкурентных продуктов просто не существует. Если вы хотите действительно избавиться от паролей и не бояться за сохранность данных, построить целостную систему безопасности вашей деловой информации в «1С:Предприятии», то «O'KEY 7.7» – единственный инструмент, который поможет вам в этом.

Усиленная аутентификация удаленных клиентов в терминальных решениях (на примере Citrix Metaframe)

С. Калачев, директор департамента разработок, Expert Mark

Передача информации в публичных сетях передачи данных. Проблематика безопасности данных.

С развитием Интернета в целом в публичных сетях передачи данных приходится достаточно часто сталкиваться с проблемой безопасности. Интернет - в прошлом и настоящем - не является безопасным местом для передачи информации. Базовые алгоритмы авторизации на серверах, предоставляющих информационные ресурсы, минимизируют нагрузку при процессе авторизации, однако не обеспечивают гарантированного определения достоверности пользовательской учетной информации.

Популярность терминальных решений. Виды современных терминальных решений.

Citrix Metaframe. Преимущества терминальных решений.

Терминальные решения, для которых характерен перенос всей вычислительной нагрузки на сервер и передача по сети только экранных форм и информации о действиях пользователя, традиционно не слишком популярны в России. Это в полной мере относится и к графическим, и тем более к текстовым терминалам. Стремление отечественных пользователей иметь непременно самую новую версию какого-либо корпоративного продукта со всем возможным технологическим арсеналом часто отождествляется с прогрессивным отношением к проблемам ИТ. На самом деле такие пользователи вовлекаются в пресловутую гонку производительности программно-аппаратных решений, часто совершенно оторванную от реальных потребностей. В итоге получается, что менее эффективные, но более экономически обоснованные решения если и используются в России, то преимущественно представительствами зарубежных компаний.

Авторизация. Проблематика гарантированного определения достоверности.

Продукт Terminal AuthPro. Назначение комплекса. USB-ключ eToken.

Аппаратная аутентификация удаленных клиентов с помощью USB-ключа eToken для решения проблемы подключения терминальных сессий к серверам на платформе Windows 2000/XP.

Предоставление для серверных приложений программного интерфейса для блокирования сессий и защищенного доступа к информации, хранящейся в USB-ключах удаленных клиентов.

Продукт Terminal AuthPro. Состав комплекса.

1. Клиентская часть, дополнительные модули к клиенту терминального сервера.
2. Серверная часть: модуль, который выполняет функции аутентификации и авторизации удаленного клиента в качестве локального пользователя на сервер Windows 2000/XP, и подключаемый модуль терминального сервера, который осуществляет защищенный обмен аутентификационной и авторизационной информацией между сервером и клиентом.
3. Средства администрирования – набор утилит, предназначенных для обслуживания репозитория клиентов системы, создания, модификации и приведения в соответствие учетной информации клиентов системы.
4. Прикладной интерфейс для серверных приложений состоит из набора функций, предназначенных для работы с удаленным клиентским eToken. Поставляется в виде SDK.

ALERO - издание и продвижение русских продуктов за рубежом

Sandra C. Desourdy, Director, ALERO Software Alliance B.V.

ПО российских производителей представляет большой интерес для западных рынков. Основная сфера деятельности компании Alero Software Alliance B.V. – «раскрутка» российских программных продуктов и решений в области защиты информации на западных рынках.

Компания предоставляет комплекс услуг по их адаптации. В их числе:

- локализация ПО с учетом стандартов страны;
- учет экспортно-импортного законодательства;
- помощь в организации технической поддержки на территории государства-экспортера.

Также Alero Software Alliance B.V. обеспечивает маркетинговое сопровождение российских продуктов и решений:

- анализ рынка государства-экспортера;
- предложение оптимальных бизнес-моделей для распространения ПО.

После проведения маркетинговых исследований компания обеспечивает издание продукта, включая:

- перевод на язык государства-экспортера;
- изготовление документации;
- полное оформление продукта (изготовление упаковки) и т.д.

Alero Software Alliance B.V. – одна из первых компаний на российском рынке, предоставляющая такие услуги российским компаниям – разработчикам ПО в области информационной безопасности.

Организация распространения программного обеспечения через Интернет по схеме Try-Before-You-Buy. Дистанционное перепрограммирование eToken

С. Груздев, генеральный директор, А. Раевский, руководитель спецпроектов, Aladdin Software Security R.D.

В последнее время ведение бизнеса активно перемещается в Интернет, с помощью которого возможна реализация нетрадиционных схем распространения/продаж ПО. Известная модель Try-Before-You-Buy реализуется так: программный продукт размещается на сайте/портале; пользователь скачивает его и, если продукт его интересует, покупает. Компания Aladdin подготовила технологическую компоненту этой схемы для компаний – участников Альянса.

Технологическая схема продаж в этом случае выглядит следующим образом. Пользователь приобретает версию какого-либо продукта вместе с электронным ключом eToken. Имея eToken, пользователь может скачать любой другой продукт и загрузить в eToken временный сертификат. При заходе на соответствующий сайт/портал и подключении eToken в ключ загружается соответствующий временный сертификат (например, на месяц) на право использования этого продукта владельцем eToken с определенным ID-номером в течении 30 дней. По прошествии месяца продукт перестает работать или переходит в режим демо-версии. При желании пользователя купить продукт он может воспользоваться уже опробованными методами (например, аналогично технологии Shareware). После оплаты информация о поступлении денег от владельца eToken с определенным ID-номером доставляется в отдел продаж. Почтовый робот автоматически отправляет заказчику письмо с сообщением о разрешении начать использовать данный продукт. Далее при входе пользователя на данный сайт/портал и подключении eToken в электронный ключ загружается цифровой сертификат, обеспечивающий пользователю неограниченную лицензию.

Таким образом, при первой покупке пользователь приобретает один из продуктов – коробочную версию – вместе с eToken, а при последующих покупках оплачивает лишь лицензию на использование программного продукта.

С помощью этой схемы реализуется обеспечение легального распространения ПО. Несмотря на то, что стоимость первичной покупки может быть довольно высока, в целом такой метод продаж представляется выгодным как для производителей/продавцов/дилеров (за счет взаимной стимуляции продаж), так и для покупателей, поскольку при последующих покупках приходится платить только за лицензию на использование продукта: покупка продукта сводится к покупке лицензии.

Инфраструктура продажи ПО через Интернет. Служба регистрации Shareware

Ф.Мучник, генеральный директор, «ТФМ и К»

На сегодняшний день в нашей стране сложилась привычная структура рынка продаж программного обеспечения: вендор, дистрибьюторы, дилеры или реселлеры, интеграторы, покупатели. В этой длинной цепочке от момента заказа программы до момента начала ее использования покупателем проходит иногда достаточно долгое время. Ведь сначала деньги должны пройти в одну сторону, и только после этого коробка с программным обеспечением – в другую сторону.

Пару лет назад мы решили оценить чужой опыт. Тогда еще в нашей стране, к сожалению, не были привычны такие термины, как электронная доставка программного обеспечения (ESD), условно-бесплатные программы (Shareware), «попробуй и купи» («try and buy»). А ведь именно при таком методе распространения программ пользователь получает продукт практически после оплаты. Конечно, структура рынка видоизменяется, появляется новое лицо – регистратор программ, своего рода посредник между вендорами, покупателями и платежными системами. Таких регистраторов во всем мире можно насчитать не более нескольких десятков, ведь на небольшой рынок программного обеспечения необходимо не более одного-двух, завоевавших доверие покупателей и вендоров.

Оценив ситуацию на нашем рынке, в начале прошлого года две фирмы («ТФМ и К» и «МКРсофт») и два онлайн-каталога программного обеспечения (www.download.ru и www.listsoft.ru) решили создать российскую службу регистрации Shareware. Для этого была создана система, которая фактически является интерфейсом между клиентами, платежными системами и авторами программ. На упомянутых сайтах и на страницах авторов программ стоят ссылки на эту систему, перейдя по которым, клиент заполняет одну простую форму и получает нужные ему реквизиты для оплаты программы. В данный момент возможны около 10 видов оплат, как для организаций, так и для частных лиц.

Достигнутые результаты говорят сами за себя – количество выписанных счетов за это время подходит к 35000, среднее количество выписанных счетов за день – около 150. Реальный процент оплачивающих – около 20-40% (в зависимости от категорий программ). Ценовой разброс – от 50 рублей до тысячи долларов.

С июля этого года этот проект получил развитие в поддержке аффилиат-программы «Лаборатории Касперского». Электронные версии антивирусного программного обеспечения любого масштаба теперь можно получить в течение одного-трех дней. Начат совместный проект по продаже «безопасной» почтовой программы The Bat! Pro (Ritlabs, «Алладин», «Лаборатория Касперского»). С запуском новой версии системы регистрации (планируется к концу года) надеемся, что количество вендоров и покупателей возрастет.

Так что рынок Shareware в России развивается не по месяцам, а по дням. Надеемся, что и наши усилия по увеличению количества продаваемых программ, разнообразия методов оплаты за их регистрацию будут достаточно заметны для российских пользователей.

Сервис-дистрибуция решений по информационной безопасности. Проект InfoSecurity.ru.

Ф. Ушаков, президент, Служба F1 – HelpNet F1 Service

Среди задач, решаемых сервисными инженерами Службы F1, можно выделить целый спектр, имеющий отношение к обеспечению информационной безопасности.

Анализ ситуации показывает, что доля таких работ имеет тенденцию к неуклонному росту, а темпы роста значительно превосходят темпы развития рынка компьютерных услуг в целом.

Перечисленные выше предпосылки определили основную цель проекта InfoSecurity.ru – формирование и расширение рынка услуг по обеспечению информационной безопасности.

Для достижения поставленных целей в рамках проекта предполагаются:

- проблемно-ориентированный сайт «Информационная Безопасность»;
- сетевая газета InfoSecurity.ru;
- услуги сертифицированных специалистов.

Проблемно-ориентированный сайт «Информационная Безопасность» служит делу популяризации идей. В рамках сайта рассматриваются проблемы, методы и решения с точки зрения сервисных инженеров, знающих реальное положение дел с обеспечением информационной безопасности в компаниях и имеющих ежедневный опыт решения задач защиты и спасения информации.

Посетитель данного ресурса может задать интересующий его вопрос или послать Запрос на обслуживание. Наиболее интересные вопросы и ответы на них предполагается публиковать в сетевой газете InfoSecurity.ru.

Сетевая газета InfoSecurity.ru – информационный бюллетень, призванный привлекать внимание общественности к данной проблеме. В каждом номере бюллетеня будут присутствовать следующие разделы: новости компаний, дайджест событий, тематические статьи и календарь событий (выставки, семинары, конференции).

Необходимость в сетевой газете InfoSecurity.ru определяется тем фактом, что к настоящему моменту освещением вопросов информационной безопасности занимаются либо СМИ компьютерной тематики, либо СМИ, посвященные вопросам безопасности целом. Как следствие, жизненно важные вопросы информационной безопасности растворяются в гуще прочих проблем, и в большинстве своем остаются незамеченными широкой общественностью.

Услуги сертифицированных специалистов.

Информационную безопасность невозможно обеспечить на практике, ограничивая данный Проект рамками СМИ. Необходима ежедневная, кропотливая работа команды сервисных инженеров. Эта команда носит название «Сервис-дистрибутор решений по информационной безопасности». Само понятие сервис-дистрибутор подчеркивает тот факт, что услуги сертифицированных специалистов не просто дополняют, а поставляются «в одном флаконе» с решениями по обеспечению информационной безопасности.

Рынок услуг по обеспечению информационной безопасности имеет одну характерную особенность. Особое внимание необходимо уделять профилактике информационной безопасности, а не доводить ИС до одного из следующих состояний: лечение вирусов, отражение атак, спасение информации или восстановление данных. Другими словами, необходимо переводить сервис по защите информации из области «чрезвычайных ситуаций» в область профилактических и плановых работ по обеспечению информационной безопасности.

Проект InfoSecurity.ru, опираясь на свои составляющие, призван и должен обеспечить информационную и сервисную поддержку решений по обеспечению информационной безопасности.

eToken Internet Logon – безопасный доступ в Интернет с защитой паролей от кражи

Ю. Илларионов, начальник отдела программных разработок, Инфотех

Программное обеспечение eToken Internet Logon обеспечивает безопасный доступ к сети Интернет, сохраняя основные параметры соединения (логин, пароль, телефоны провайдера) в защищенной области электронного ключа eToken.

Для работы с eToken Internet Logon необходимо наличие:

- PC с USB-портом и ОС Windows 95/98/ME/NT4/2000;
- установленного модема;
- электронного ключа eToken R2.

eToken Internet Logon замещает вызов стандартного драйвера Microsoft, перехватывая на уровне реестра обращение к классам .DUN и .PBK. При этом происходит передача системе параметров соединения, считанных из памяти электронного ключа. Отметим, что все основные параметры (и главное – пароль) не хранятся в компьютере, что делает их похищение хакерскими методами практически невозможным.

Система eToken Internet Logon использует следующие понятия:

1. PIN-код: код для входа в ключ (может изменяться клиентом, но не может быть прочитан из ключа). Отметим, что похищение PIN-кода ничего не даст злоумышленнику, ибо для работы в Интернете под логином клиента ему придется похитить еще и сам ключ.
2. Логин и пароль для доступа в Интернет. Эти параметры хранятся в ключе и клиенту не нужно их запоминать или записывать. Достаточно указать только PIN-код при установлении соединения с Интернетом, и система автоматически подставит все необходимые параметры, прочитав их из ключа.

Основной гарантией безопасности является постоянное наличие ключа при клиенте (габариты позволяют). При подозрении, что кто-то узнал PIN-код, достаточно просто поменять его с помощью программы-редактора. В случае похищения ключа необходимо немедленно сообщить об этом провайдеру сети и попросить его сменить пароль. В обоих случаях клиент гарантирован от работы злоумышленника в сети за его (клиента) счет.

Для установки программы необходимо вставить в дисковод прилагаемый компакт-диск и перейти в его корневую директорию. После этого надо запустить программу setup.exe и следовать ее указаниям. Единственный вопрос, на который нужно будет ответить – это указать директорию, в которую будут скопированы файлы системы eToken Internet Logon. По умолчанию это c:/Program Files/ eToken Internet. После установки система готова к работе.

Secret Disk – сертифицированная система защиты конфиденциальной информации

А. Куприянов, руководитель отдела корпоративных проектов, Aladdin Software Security R.D.

Логин и пароль нередко представляются надежными средствами для защиты информации. Однако они служат лишь для разграничения доступа к данным, тогда как сами информационные ресурсы хранятся на жестком диске компьютера в открытом, незащищенном виде. Особенному риску при этом подвергаются данные, хранящиеся на винчестерах переносных компьютеров. Secret Disk – система, обеспечивающая одновременно возможность защитить данные сразу тремя способами, позволяя:

- организовать разграничения доступа к ресурсам (при этом используется двойная, аппаратно-программная, идентификация);
- зашифровать конфиденциальные данные;
- скрыть их наличие.

Принцип работы.

Secret Disk создает «секретные» логические диски. При сохранении на них информация автоматически шифруется. Доступ к ресурсам осуществляется с помощью аппаратного ключа и пароля. С секретными дисками могут работать несколько пользователей; для этого у каждого из них должен быть свой ключ и пароль.

Возможности.

1. Безопасная работа, хранение и передача конфиденциальной информации.
2. Аппаратная идентификация пользователей.
3. Возможность использования мощных криптоалгоритмов (подключение средств криптографической защиты, например, входящих в поставку Windows или эмулятора платы «Криптон» фирмы «АНКАД» с мощным российским алгоритмом шифрования с длиной ключа 256 бит).
4. Мгновенное «уничтожение» информации при сигнале «тревога» или входе «под принуждением».
5. Блокирование компьютера в перерывах между работой.
6. Создание защищенных архивов (в том числе для пересылке по почте, хранения на магнитных носителях).
7. Простота и удобство в работе.

Преступления в сфере компьютерной информации. Опыт борьбы на примере Перми и Пермской области

О. Искандаров, начальник отдела по борьбе с преступлениями в сфере компьютерной информации и контрафактным программным обеспечением, «Управление Р» при ГУВД Пермской области

В связи с развитием высоких технологий в последние годы обозначилось новое направление преступлений, имеющих не только тенденцию увеличения по количеству, но и все более сложных в исполнении.

К преступлениям в сфере компьютерной информации Уголовное право России относит деяния, предусмотренные статьями 272, 273, 274 УК РФ.

Перечень наиболее характерных преступлений:

- копирование, блокирование, модификация охраняемой Законом информации;
- распространение вредоносных программ, если это повлекло за собой копирование; блокирование или модификацию охраняемой Законом информации;
- блокирование работы ЭВМ, системы ЭВМ или их сетей.

Наиболее типичные преступления в сфере компьютерной информации в Пермской области:

- кража информации о паролях доступа в Интернет у клиентов интернет-провайдеров;
- распространение вредоносных программ типа «троянский конь»;
- распространение контрафактных копий программного обеспечения и аудиовизуальных произведений.

Проблемы, с которыми сталкиваются правоохранительные органы в борьбе с преступлениями в области компьютерной информации:

- высокая латентность преступлений в сфере компьютерной информации;
- нежелание руководителей предприятий, учреждений и организаций выступать в качестве пострадавших в уголовных делах;
- низкий уровень квалификации сотрудников органов правопорядка в сфере IT;
- низкий уровень оснащённости органов правопорядка техническими средствами;
- отсутствие представителей, правообладателей и разработчиков ПО;
- отсутствие четко налаженного механизма привлечения виновных к ответственности.

Любая информация, которая представляет ценность, должна быть защищена. Опыт показывает, что эффективной может быть только комплексная защита.

Управление безопасностью в корпоративных информационных системах: eSafe - комплексная технология защиты информации

И. Ляпунов, начальник отдела систем информационной безопасности, ЛАНИТ

Комплексный подход — важнейший принцип управления безопасностью

Возрастающая сложность корпоративных информационных систем (ИС), увеличение числа используемых системно-технических платформ и сетевых сервисов приводит к расширению списка уязвимостей и повышает требования к средствам защиты. Появляется большое количество новых типов атак на ИС и, соответственно, новых передовых технологий защиты. Использование стандартных средств защиты, таких как межсетевые экраны, виртуальные частные сети, средства защиты от несанкционированного доступа, — необходимое, но уже не достаточное условие построения надежной и эффективной системы информационной безопасности. Решить эту проблему позволяет проведение полного цикла работ по построению комплексной системы информационной безопасности, включающего обследование всей «информационной жизни» компании-заказчика, ее бизнес-процессов, документальных и информационных потоков, серверного парка, сетевого оборудования, программного обеспечения и т.д., разработку концептуальных решений, комплекса организационных, процедурных и программно-аппаратных мер защиты, внедрение выбранных технологий и их взаимную «стыковку», обучение персонала, сопровождение системы.

Сложный развивающийся организм, имеющий своей главной целью обеспечение безопасности организации, ее информации и информационных потоков, обладает сложной внутренней структурой, действующий по своим собственным законам. В связи с этим возникает проблема контроля этого организма. С появлением новых технологий защиты, усложнением существующих, а также ростом самой корпоративной информационной системы остро встает вопрос управления безопасностью. Идеология управления безопасностью закладывается еще на этапе разработки Концепции информационной безопасности, проектирования системы защиты информации.

eSafe — новая технология защиты информации при работе в Интернете

Система защиты корпоративных ресурсов для серверов NT/2000/NetWare **eSafe Enterprise** обеспечивает комплексный аудит информации и контроль всех рабочих станций из одной точки, в реальном времени проверяет все входящие файлы, Java и ActiveX-апплеты, скрипты и присоединенные файлы электронной почты на наличие вредоносной активности, а также защищает конфиденциальные данные от случайного или преднамеренного копирования или отправки через Интернет.

eSafe Gateway защищает корпоративные сети от проникновения любого нежелательного содержимого, предотвращает кражи конфиденциальной информации на уровне интернет-шлюзов и может работать как вместе с Firewall, так и автономно. Весь трафик по протоколам FTP, HTTP, SMTP в реальном времени очищается от вирусов и вредоносных скриптов, ActiveX и Java-апплетов. Сканируются входящие и исходящие файлы, электронные сообщения с присоединенными файлами, документы MS Office, все типы MIME и все форматы сжатых данных.

eSafe Mail обеспечивает комплексную и гибкую систему защиты почтовых серверов SMTP, а также серверов групповой работы типа MS Exchange или Lotus Notes.

Защита от искажения и подделки информации в Интернете. Цифровые сертификаты Thawte

А. Глазков, заместитель технического директора, РосБизнесКонсалтинг

Необходимость защиты информации от просмотра и фальсификации. Задачи современных систем защиты.

Основные технологии, уровни защиты и их связь с сетевыми уровнями и интернет-протоколами. Криптозащита на различных уровнях, преимущества и недостатки.

История SSL и базовые принципы. Взаимодействие протокола SSL с другими интернет-протоколами. Проблемы работы в открытой сети с маршрутизацией пакетов.

Основные функции SSL-протокола – аутентификация сторон, шифрование, целостность данных.

Схема работы сертификатов. Обмен данными между сервером, браузером и центром сертификации. Структура данных в сертификате. Процесс установления соединения и механизм использования открытых, закрытых, сеансовых ключей и хэширования в протоколе SSL.

Крупнейшие системы SSL-сертификатов. История, рыночные сегменты. Виды сертификатов по назначению и стойкости. Преимущества систем.

Предлагаемые на российском рынке варианты.

Критерии и причины выбора провайдера холдингом РосБизнесКонсалтинг. Продажи SSL-сертификатов. Реальные и потенциальные заказчики и их потребности.

Использование SSL-сертификатов в разработках РосБизнесКонсалтинга – сайты, интернет-магазины, страховые компании, дистрибьюторские компании, службы публикации новостей, почтовые системы, интранет-системы.

Пути повышения надёжности и удобства систем защиты информации на базе SSL-сертификатов. Варианты хранения ключей, их преимущества и недостатки. Возможности и желательность интеграции с аппаратными средствами защиты информации. Основные функции современных электронных ключей. Реальное использование электронных ключей в РосБизнесКонсалтинге.

Особенности современных PKI-систем. RSA Keon Advanced PKI

Р. Кашапов, системный инженер отдела информационной безопасности, Demos

1. Современные PKI-системы.

PKI-системой называется система, в которой реализована возможность управления ключами для обеспечения требуемого уровня безопасности. В современных PKI-системах это реализовано посредством управления цифровыми сертификатами. При проектировании PKI-систем важной частью является разработка политики выдачи сертификатов и их использования. Кроме того, необходимо позаботиться об организации публичного доступа к сертификатам, возможности аннулирования сертификатов, восстановления устаревших/аннулированных ключей. При выборе PKI-системы нужно обратить внимание на поддержание ею уже имеющихся стандартов. Это даст возможность «прозрачной» работы с внешними по отношению к системе пользователями. Наличие сервера сертификатов не является достаточным основанием для того, чтобы продукт можно было назвать PKI-системой.

2. Расширенные возможности PKI-систем.

Keon Advanced PKI – это PKI-решение, предоставляемое компанией RSA Security. Оно состоит из следующих компонентов: сервер безопасности (Keon Security Server) – центральная часть системы Keon. Именно сервер безопасности предоставляет сервисы по аутентификации, авторизации, проверке подлинности сертификатов, управлению правами доступа в системе и централизованный журнал событий. Рабочий стол (Keon Desktop) – пользовательская компонента системы; предоставляет услуги по шифрованию файлов, созданию защищённых областей на диске, в том числе для групп, и доступ к защищённому приложению. Keon-агенты используются для безопасного доступа к серверам приложений. Keon-агент совместно с Рабочим столом обеспечивает шифрование сессии, ведение централизованного журнала событий, автоматическую аутентификацию пользователей. Кроме того, RSA Keon advanced PKI на этапе входа в систему позволяет использовать преимущества двухфакторной аутентификации. Это может достигаться двумя путями.

1. Использование смарткарт; смарткарта, в свою очередь, защищается PIN-кодом.

2. Использование технологии RSA SecurID.

Технология RSA SecurID позволяет аутентифицироваться при помощи PASSCODE, который состоит из PIN (известного лишь обладателю) и значения аппаратно получаемого числа, изменяющегося каждую минуту.

При отсутствии готового агента имеется возможность его создания при помощи специализированных библиотек разработчика.

Инфраструктура открытых ключей на основе Baltimore UniCERT

С. Знаменский, технический консультант, Hewlett-Packard

Стратегия HP на создание и развитие безопасных интернет-технологий.

Обзор нового семейства программных продуктов HP Netaction, включающего инструментарий разработки, внедрения и интеграции новейших решений.

HP PKI – важный компонент в ряду продуктов для обеспечения информационной безопасности семейства HP Netaction.

Рассматриваются задачи обеспечения информационной безопасности, их решение с использованием программных продуктов HP Netaction, а также Программное решение HP PKI (OEM Baltimore UniCERT) как средство построения инфраструктуры открытых ключей.

Достоинства программного решения HP PKI (UniCERT).

Решение задач защиты данных, пересылаемых по незащищенным каналам сети общего доступа – Интернет (обеспечение целостности данных, конфиденциальности, разграничение доступа, цифровая подпись) с помощью программного решения HP PKI.

Компоненты программного решения HP PKI (UniCERT).

Описание компонентов программного решения HP PKI и способов построения инфраструктуры открытых ключей с их помощью.

Примеры комплексных решений HP, использующих технологию HP PKI.

Защищенный клиент Check Point SecuRemote VPN-1.

Сертифицированное OPSEC решение

И. Кораблев, системный инженер, Безопасные Информационные Технологии

В настоящее время предприятия уже не ограничиваются стенами одного офиса. Возникает реальная опасность несанкционированного доступа к информации в момент передачи ее по каналам, находящимся вне границ, контролируемых организационно-административными мерами предприятия.

Наиболее дешевым, легко внедряемым и гибким средством на сегодняшний день является технология построения виртуальных частных сетей (ВЧС). Данная технология позволяет формировать защищенные каналы передачи информации в сетях общего пользования (например, Интернет), которые в настоящее время являются легко доступными из любой точки земного шара.

В данный момент рынок уже наполнен средствами построения ВЧС, однако унифицированное решение по построению ВЧС еще не разработано и не принято в качестве стандарта. Поэтому необходимо четко осознавать требования, которым должно соответствовать средство ВЧС.

В результате анализа функций, возлагаемых на средства ВЧС, очевидно, что данное средство должно быть легко интегрируемым с другими средствами обеспечения информационной безопасности. Для этого средство ВЧС должно поддерживать все основные стандарты и протоколы, направленные на обеспечение безопасности информации. Так же средство ВЧС должно легко накладываться на любые гетерогенные сети любой топологии.

В качестве примера рассмотрим средство ВЧС VPN-1/FireWall-1 компании Check Point Software Technologies. Данное средство предоставляет максимум возможностей среди аналогичных ему продуктов. Оно поддерживает наибольшее количество открытых стандартов и протоколов и позволяет легко интегрировать его с любыми другими средствами обеспечения информационной безопасности.

Данное средство предоставляет возможность подключения удаленных пользователей к корпоративной виртуальной частной сети посредством использования клиентов VPN-1 SecuRemote, что позволяет авторизованному сотруднику получать необходимую информацию по защищенному каналу из любой точки земного шара.

Для усиления безопасности удаленного доступа необходимо использовать аппаратные средства аутентификации. Примером является продукт VPNkey, который является результатом интеграции клиента удаленного доступа VPN-1 SecuRemote и электронного USB-ключа eToken компании Aladdin. Данный продукт позволяет усилить устаревшую систему парольной идентификации до современного уровня и использовать аутентификацию на основе сертификатов, используя отчуждаемый носитель ключевой информации, который легко займет место брелка на связке обычных ключей.

Безопасное подключение локальных сетей к открытым ресурсам Интернет на базе технологий VPN

В. Игнатов, вице-президент, ИнфоТеКС

Технология определяет три типовых случая подключения локальной сети к Интернет и реализуется на базе пакета программ «ViPNet» компании ИнфоТеКС, имеющего сертификаты Гостехкомиссии и ФАПСИ.

1. Подключение локальной сети к Интернету для организации работы отдельных станций локальной сети с открытыми ресурсами Интернета.

Технология ориентирована:

- на создание в локальной сети для трафика Интернета защищенных «туннелей» от входа сети непосредственно до станций, подключаемых к Интернету;
- реализацию альтернативной логики работы станций, подключаемых к Интернету:
 - либо с Интернета с блокировкой любого трафика в локальную сеть,
 - либо в локальной сети с блокировкой «туннелей» в Интернет;
- организацию режимов односторонних соединений с открытыми ресурсами и фильтрацию поступающего трафика по различным параметрам путем комбинации свойств межсетевых и персональных сетевых экранов;
- обнаружение и блокирование незарегистрированных программ – «Троянов», пытающихся несанкционированно собрать или передать любую информацию.

2. Подключение локальной сети к Интернету для защищенного взаимодействия локальной сети или отдельных ее компьютеров с другими локальными сетями или отдельными компьютерами.

Технология ориентирована:

- на создание защищенных «туннелей» через Интернет между локальными сетями или непосредственно их компьютерами, а также до отдельных рабочих станций или мобильных компьютеров в Интернете;
- блокировку любого входящего и исходящего открытого трафика вне защищенных «туннелей» на границе локальных сетей или компьютеров;
- возможность создания в локальной и глобальной сети замкнутых или частично пересекающихся групп пользователей и серверов;
- использование персональных сетевых экранов при работе в локальной сети.

3. Комбинированная схема, сочетающая оба предыдущих случая.

Все технологические решения реализуются путем установки на компьютерах в различных комбинациях ПО ViPNet-клиент и ViPNet-координатор, обеспечивающих прозрачное шифрование любого IP-трафика, а также выполнение указанных выше и многих других функций. Конфигурация и управление виртуальной защищенной сетью осуществляется с использованием ПО Центра управления сетью и ключевого центра.

Комбинированная ключевая структура сочетает симметричную и асимметричную схему распределения ключей с использованием процедур ЭЦП.

Технологии защиты от несанкционированного доступа в клиент-серверных приложениях. Система Matrix

М. Кириллов, начальник отдела проектирования, ЛАНИТ

Корпоративные прикладные системы нуждаются в надежной защите от несанкционированного доступа (НСД). Что требуется от системы разграничения доступа? Необходимо однозначно идентифицировать субъекта, пытающегося войти в систему, и проверить его подлинность. Для успешно авторизованного пользователя необходимо настроить интерфейс клиентского рабочего места в соответствии с правами, указанными в матрице доступа. Перед тем как выполнить запрашиваемую пользователем операцию приложение должно связаться с сервером доступа с целью проверки полномочий данного пользователя системы на операцию. Все попытки выполнения операций, доступ к которым разграничивается, могут протоколироваться в журнале безопасности.

ЛАНИТ разработал систему *Matrix* для решения задачи разграничения доступа в корпоративных системах. Основные возможности системы следующие.

- Администратор информационной безопасности с помощью графического интерфейса *Matrix* сможет управлять доступом к операциям в системах клиент-сервер, используя такие термины, как: пользователь, служебная обязанность, технологическая операция в программе. Администратору безопасности нет необходимости досконально разбираться в архитектуре защищаемой системы, которая состоит из множества разнородных объектов, связанных между собой алгоритмическими функциями. Администратору безопасности не придется оперировать такими понятиями, как право вставки записи в таблицу, право на запуск процедуры, право модификации файла и т.д. Все внутреннее устройство программ будет скрыто за набором интуитивно понятных технологических операций.
- Разработчики корпоративных систем смогут существенно снизить трудоемкость процесса выполнения требований по защите информации и повысить защищенность своих систем. Разработчику нужно будет лишь вставить в свой код обращение к функциям API *Matrix* и описать в базе данных *Matrix* все операции в своей системе, доступ к которым должен быть разграничен.
- Для того, чтобы соблюдать установленные правила безопасности, пользователям корпоративных систем, защищаемых *Matrix*, не надо будет запоминать сложных паролей и заботиться об их периодической смене. Пользователю достаточно будет вставить электронный брелок eToken компании Aladdin в разъем компьютера, либо коснуться большим пальцем руки окошка мыши BioLink со встроенным сканером, и *Matrix* сможет идентифицировать пользователя и определить все доступные для него элементы интерфейса. При этом повышается защищенность системы и удобство работы.

Разработанное компанией ЛАНИТ программное обеспечение *Matrix* позволит в кратчайшие сроки интегрировать готовые механизмы разграничения доступа к информации в создаваемые прикладные системы.

Презентация Novell NetWare 6.0

М. Елашкин, А. Жерлицын, К. Степанов, Novell

Впервые в России представлена последняя версия сетевой операционной системы NetWare 6. NetWare 6 – это больше, чем просто следующая версия NetWare; это возможность для компании внести значительные изменения в ведение своего бизнеса.

NetWare 6 обеспечивает бесперебойный защищенный доступ к сетевой информации вне зависимости от ее местонахождения. NetWare 6 решает многие из сегодняшних проблем, с которыми сталкиваются большинство организаций, в частности:

- увеличение количества сотрудников организации;
- увеличение числа сотрудников, пользующихся удаленным или мобильным доступом к корпоративным данным;
- необходимость обеспечения защищенного доступа для партнеров и поставщиков к корпоративным данным через Интернет;
- потребность в большем количестве разделяемых сетевых ресурсов для хранения данных;
- необходимость использования технологии SAN;
- потребность в постоянном доступе к сетевым службам (печать, хранение файлов, почта, приложения), включая доступ через Интернет;
- максимально эффективное использование многопроцессорных серверов;
- резервное копирование корпоративных данных, включая данные мобильных пользователей;
- уменьшение стоимости владения и увеличение отдачи от информационных технологий.

Secret Disk Server – система «прозрачного» шифрования томов NetWare с возможностью мгновенного отключения. Защищенный BackUp

А. Бевз, технический эксперт, Aladdin Software Security R.D.

Как показывает опыт, большинство пользователей считают себя защищенными, если для входа в систему используются логин и пароль. На самом деле при вводе пароля осуществляется лишь разграничение доступа к информационным ресурсам, которые при этом хранятся на сервере в незащищенном, открытом виде. Задача защиты информации имеет две составные части: ограничение доступа к информационным ресурсам и собственно их защита. Второе обеспечивается шифрованием.

Количество продуктов, обеспечивающих разграничение доступа, достаточно велико. Secret Disk Server – одно из немногих средств для шифрования информационных ресурсов. С его помощью информация, хранящаяся на сервере, становится действительно надежно защищенной.

1. Secret Disk Server для Novell NetWare 4.11-5.x как составная часть линейки программных продуктов по защите информации с помощью шифрования «на лету».
2. Особенности реализации Secret Disk Server для Novell NetWare 4.11-5.x (SDS NW).
3. Принцип работы SDS NW.
4. Управление защищенными томами.
5. Управление ключами в системе.
6. Запуск системы.
7. Сигнал «Тревога».
8. Система защищенного резервного копирования данных на серверах Novell NetWare.
9. Новые криптопровайдеры. Интеграция с программным эмулятором платы «Криптон» (платформа NLM) фирмы «Анкад».
10. SDS NW – открытая система для использования алгоритмов криптопреобразования сторонних разработчиков.

Усиление серверных процедур идентификации и аутентификации NDS eDirectory и BorderManager и контроль их целостности. Защищенные клиенты Trusted Login

Г. Лебедев, технический эксперт, А. Шакуов, научный консультант, БИТС

Дается описание реализованных в рамках OTNA подсистем усиленной идентификации и аутентификации в гетерогенной среде защищенных иерархических компьютерных систем на базе программно-аппаратных платформ типа eToken, Touch Memory, Smart Card и т.п.

Многоуровневая среда управления безопасностью корпоративных систем в гетерогенных сетях

А. Шакуов, научный консультант, БИТС

Дается анализ реализованных и апробированных защищенных иерархических компьютерных систем на базе гетерогенных программно-аппаратных платформ.

В качестве *базовой реализации* унифицированных интерфейсов безопасности автоматизированных систем – The Uniform Trusted Interfaces Concept (UTIC) разработан комплекс «Система защиты с открытой архитектурой для Автоматизированных Систем, функционирующих в среде гетерогенных сетей – Open Trusted Network Architecture» (OTNA). Описание применения OTNA дает более детальное представление и обо всей архитектуре UTIC.

Комплекс «Система защиты с открытой архитектурой Автоматизированных Систем, функционирующих в среде гетерогенных сетей – Open Trusted Network Architecture» (OTNA).

Назначение. Комплекс OTNA – многоуровневая среда управления безопасностью корпоративных автоматизированных систем, построенных на базе гетерогенной корпоративной сети.

Основные характеристики. Комплекс OTNA построен по модульному принципу и состоит из следующих базовых подсистем:

- Trusted DirectoryNet (TDN) – базовая реализация подсистемы THN архитектуры UTIC;
- Trusted Client Unit (TCU) – базовая реализация подсистемы Trusted Client архитектуры UTIC;
- Trusted BorderManager (TBM) – базовая реализация подсистем Trusted FireWall и Trusted VPN; архитектуры UTIC
- Trusted GroupWise (TGW) – базовая реализация подсистемы Trusted Post System архитектуры UTIC

Комплекс OTNA обеспечивает защиту корпоративных АС, построенных на гетерогенных сетях, включающих следующие сетевые платформы:

- NetWare 4.x, 5.x;
- Windows NT 4.0 Server, Windows 2000 Server;
- Linux;
- FreeBSD;
- HP-UX;
- IBM AIX;
- IBM MVS;
- IBM OS/390;
- Sun Solaris (SPARC и Intel платформы);
- Tru 64 Unix.

Все подсистемы OTNA имеют сертификаты Гостехкомиссии РФ.

Тел.: (095) 231-3113
e-mail: conf@aladdin.ru
Web: www.aladdin.ru/conf

Спонсоры:

Microsoft®

Novell®

ALERO
SOFTWARE B.V.

ALADDIN®
SOFTWARE SECURITY R.D.