ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. КОМПЛЕКСНЫЙ ПОДХОД

Малёжин Олег Борисович
директор департамента ОАО "Элвис-Плюс"

"Нефтяное хозяйство"
№9, 2001

Введение

Проблема обеспечения информационной безопасности предприятий в настоящее время стала крайне актуальной. Более того, не только зарубежные, но уже и отечественные предприятия и организации в полной мере вкусили горьких плодов недооценки этой проблемы, и потому подписание Президентом РФ "Доктрины информационной безопасности России" воспринима ется как знак понимания и озабоченности существованием такой проблемы руководством страны. Как указывается в "Доктрине …": "Воздействию угроз информационной безопасности РФ в сфере экономики наиболее подвержены:

- системы бухгалтерского учета предприятий … независимо от формы собственности;
- системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации …".

Указанная проблема затрагивает любую организацию, имеющую хотя бы несколько компь ютеров независимо от ее масштабов и принадлежности к тому или иному сектору экономики. Именно признанием существования проблемы и необходимостью ее решения и продиктовано включение в повестку дня 29-ой ежегодной конференции "Современные информационные технологии в нефтяной промышленности" отдельного раздела "Информационная безопас ность".

Из чего складываются финансовые потери организаций?

Отечественная статистика в настоящее время не в состоянии ответить на вопрос "какие фи нансовые потери несут отечественные организации от компьютерных преступлений?", поэтому обратимся к зарубежной статистике.

Так, по данным ФБР США, в течение последних двух лет 78% опрошенных компаний понес ли финансовые убытки, связанные с недостаточной информационной безопасностью. Основ ные причины потерь:

- 76% компаний, понесших убытки, пострадали от компьютерных вирусов (убытки аме риканского бизнеса в 1999 г. от эпидемий вирусов Melissa, ExploreZip и т.п. оцениваются в $7.6 миллиардов долларов);
- 42% - от атак изнутри;
- 25% - от атак извне;
- 70% компаний пострадали от ошибок невнимательности;
- 10% - от промышленного шпионажа.

Что означает комплексный подход в применении к области информационной безопасности предприятия?

Понятно, что в зависимости от масштаба организации методы и способы обеспечения ин формационной безопасности могут различаться, но любой руководитель и специалист знают, что практически любая техническая проблема не поддаётся одностороннему решению, а все гда требует комплексного подхода. Однако, ввиду некоторой новизны проблематики инфор мационной безопасности, у многих реально заинтересованных лиц превалирует однобокий подход. В настоящее время с сожалением приходится констатировать, что ситуация в области проблематики информационной безопасности осознается многими ответственными работни ками таковой, что позволяет решить все проблемы в этой сфере, не прилагая особых организа ционных, финансовых и технических усилий.

Нередко со стороны людей, позиционирующих себя в качестве ИТ-специалистов, приходится слышать мнения типа "проблемы информационной безопасности в нашей компании мы реши ли - мы установили межсетевой экран" (вариант: "мы купили 10 лицензий на средства антиви русной защиты").

Такой подход свидетельствует, что существование проблемы уже признается, но сильно не дооценивается ее масштаб и насущность, и, как следствие, недооцениваются масштаб и слож ность совершенно необходимых срочных мероприятий по ее решению. В тех же компаниях, где руководство и специалисты всерьез задумались над тем, как обезопасить свой бизнес и из бежать финансовых потерь, признано, что одними локальными мерами типа оснащения кор поративных информационных систем в достаточном количестве межсетевыми экранами или антивирусными средствами уже не обойтись, а нужно применять именно комплексный под ход. К финансовым потерям вследствие отсутствия информационной безопасности можно от нести, например:

- особенности конкурентной борьбы;
- недобросовестность сотрудников, клиентов и партнеров;
- отсутствие разграничения доступа к различным информационным ресурсам;
- "любознательность" хакеров;
- обилие вирусов, которые не признают не только географических границ, но и границ между корпоративными сетями и сетями общего пользования и т.д.;

С чего начать?

Начальным этапом комплексного подхода следует считать этап разработки "политики ин формационной безопасности".

Основные цели "политики …":

I. анализ реальных угроз для корпоративной информационной системы, зависящих от таких существенных параметров, как:

1. сфера деятельности компании и, как следствие, определение соотношения инициро ванных злоумышленниками и спонтанных (например, техногенного характера) угроз;
2. перечня, уровня и источников приобретения компанией информационного, вычисли тельного и коммуникационного оборудования, а также используемого программного обес печения;
3. существующего в компании режима организации доступа персонала к информацион ным ресурсам и уровня контроля соблюдения такого режима сотрудниками компании;
4. формирование рекомендуемого "периметра безопасности" компании, исходя из соотноше ния уровней:

- ущерба от возможной реализации угроз различным сегментам корпоративной информа ционной сети;
- затрат, требуемых для её защиты на установленном уровне;
- оценка ущерба в случае непринятия как полного комплекса рекомендованных средств и мероприятий, так и частных решений и рекомендаций;

II. предложение оптимальных вариантов защиты, дифференцируемых в зависимости от:

1. уровня конфиденциальности или коммерческой ценности той или иной корпоративной информации;
2. состава различных категорий пользователей и режима их доступа к корпоративным ин формационным ресурсам;
3. множества иных критичных факторов.

От теории к практике

Следующим логичным шагом после разработки политики информационной безопасности следует считать определение комплекса средств, предполагаемых к использованию в процессе реализации выработанной ранее "политики…".

Типовой набор средств защиты должен включать в себя следующие компоненты:

- средства защиты от вирусов с использованием специализированных комплексов анти вирусной профилактики;
- средства разграничения доступа к информационным ресурсам, а также защита от не санкционированного доступа (НСД) к информации с использованием технологии токенов (смарт - карты, touch-memory, ключи для USB-портов и т.п.);
- средства обеспечения надежного хранения информации с использованием технологии защиты на файловом уровне (кодирование файлов и каталогов);
- средства защиты от внешних угроз при подключении к общедоступным сетям связи (например: Internet), а также средства управления доступом из сети Internet с использовани ем технологии межсетевых экранов (Firewall) и содержательной фильтрации (Content Inspection);
- средства обеспечения конфиденциальности, целостности и подлинности информации, передаваемой по открытым каналам связи с использованием технологии VPN (защищенных виртуальных частных сетей);
- средства обеспечения активного исследования защищенности информационных ре сурсов с использованием технологии Intrusion Detection (обнаружение атак);
- средства обеспечения централизованного управления системой информационной безопасности в соответствии с согласованной и утвержденной политикой безопасности.

О многих компонентах информационной безопасности написано много статей, некоторым же компонентам не уделяется должного внимания, видимо в силу их новизны. Остановимся под робнее на некоторых аспектах применения средств информационной безопасности, которые относительно обойдены вниманием. Заметим, что с учетом многообразия средств обеспечения информационной безопасности одной компании, какой бы разносторонней не была область ее деятельности, не под силу разработка всего разнообразия средств защиты. Исходя из этого, наша

компания исповедует принцип применения собственных разработок, а также разработок компаний-партнеров.

1. Антивирусные средства

Лавинообразным распространением вирусов действительно напуганы многие (в настоящее время известно более 45000 компьютерных вирусов и каждый месяц появляется более 300 но вых разновидностей). При этом считается, что основной путь "заражения" компьютеров - через Интернет, поэтому наилучшее решение, по мнению многих, отключить сеть от этой паутины. Есть Интернет - есть проблемы, нет Интернета - нет проблем. При этом забывается, что суще ствует множество других путей проникновения вирусов на конкретный компьютер, например:

- пиратское программное обеспечение;
- персональные компьютеры "общего пользования" (например, опасность представляют домашние компьютеры, если на них работает более одного человека).

2. Технологии токенов (смарт-карты, touch-memory, ключи для USB-портов)

Электронные токены являются средством повышения надежности защиты данных на основе гарантированной идентификации пользователя. Токены являются так называемыми "контейнерами" для хранения персональных данных пользователя системы. Основное пре имущество электронного токена заключается в том, что персональная информация всегда на ходится на носителе (смарт-карте, ключе и т. д.) и предъявляется только во время доступа к системе или компьютеру.

Одна из проблем, которая начинает ощущаться в настоящее время, заключается в том, что считается "хорошим тоном" использование токенов для разнообразных задач (шифрация ин формации на прикладном уровне, на сетевом уровне, доступ к компьютеру или к отдельным приложениям и т.д.). Поэтому пользователь в конечном итоге "обрастает" разнообразными то кенами, а ему нужен один, но универсальный токен…

3. Защита информации на файловом уровне

Эти технологии позволяют скрыть конфиденциальную информацию пользователя на жест ком диске компьютера или на сетевых дисках путем кодирования содержимого файлов, ката логов и дисков. Доступ к данной информации осуществляется по предъявлению ключа, кото рый может вводиться с клавиатуры, храниться и предоставляться со смарт-карты, HASP- или USB-ключей и прочих токенов. Помимо вышеперечисленных функций указанные средства по зволяют мгновенно "уничтожить" информацию при подаче сигнала "тревога" и при "входе под принуждением", а также блокировать компьютер в перерывах между работой.

4. Межсетевые экраны

Использование технологии межсетевых экранов предлагается для решения таких задач как

- безопасное взаимодействие пользователей и информационных ресурсов, расположен ных в Extranet- и Intranet-сетях, с внешними сетями;
- создание технологически единого комплекса мер защиты для распределенных и сег ментированных локальных сетей подразделений предприятия;
- построение иерархической системы защиты, предоставляющей адекватные средства обеспечения безопасности для различных по степени закрытости сегментов корпоративной сети.

В зависимости от масштабов организации и установленной политики безопасности в органи зации, рекомендуются межсетевые экраны, отличающиеся по стоимости и степени функцио нальности как собственной разработки, так и разработки других производителей (межсетевой

экран собственной разработки ЗАСТАВА, межсетевой экран CheckPoint Firewall-1, межсетевой экран Private Internet Exchange (PIX) компании Cisco).

5. Защищенные виртуальные частные сети

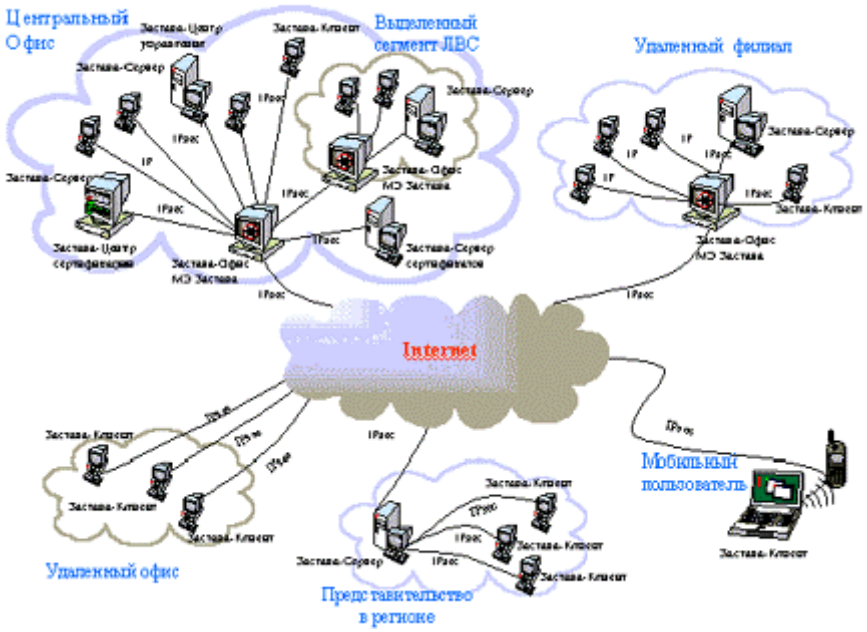
Для защиты информации, передаваемой по открытым каналам связи, поддерживающим про токолы TCP/IP, мы предлагаем ряд программных продуктов ЗАСТАВА, предназначенных для построения защищенных виртуальных частных сетей (VPN) на основе международных стан дартов IPSec.

Продукты работают в операционных системах Windows 95/98/NT и Solaris и обеспечивают:

- защиту (конфиденциальность, подлинность и целостность) передаваемой по сетям информации;
- контроль доступа в защищаемый периметр сети;
- идентификацию и аутентификацию пользователей сетевых объектов;
- централизованное управление политикой корпоративной сетевой безопасности.

При этом:

- Открытый криптоинтерфейс позволяет использовать различные реализации криптоалго ритмов, что приводит к возможности использования продуктов в любой стране мира в со ответствии с принятыми национальными стандартами;
- Наличие в семействе ЗАСТАВА разнообразных модификаций (линейка продуктов включает 9 наименований для клиентских, серверных платформ, для сети масштаба офиса, для генерации ключевой информации) позволяет подбирать оптимальное по стоимости и надежности решение с возможностью постепенного наращивания мощности системы защиты



6. Технологии обнаружения атак (Intrusion Detection)

Постоянное изменение сети (появление новых рабочих станций, реконфигурация программ ных средств, и т.п.) может привести к появлению новых уязвимых мест, угроз и возможностей атак как на информационные ресурсы, так и на систему защиты. В связи с этим особенно важ но своевременное их выявление и внесение изменений в соответствующие настройки инфор

мационного комплекса и его подсистем, и в том числе, в подсистему защиты. Это означает, что рабочее место администратора системы должно быть укомплектовано специализированными программными средствами обследования сетей и выявления уязвимых мест (наличия "дыр") для проведения атак "извне" и "снаружи", а также комплексной оценки степени защищенности от атак нарушителей.

В состав комплексного предложения ЭЛВИС+ входят наиболее мощные среди обширного семейства коммерческих пакетов продукты компании Internet Security Systems (Internet Scanner и System Security Scanner), а также продукты компании Cisco: система обнаружения несанк ционированного доступа NetRanger и сканер уязвимости системы безопасности NetSonar.

7. Инфраструктура открытых ключей (PKI)

Основными функциями PKI являются: поддержка жизненного цикла цифровых ключей и сертификатов (т.е. их генерация, распределение, отзыв и пр.), поддержка процесса идентифи кации и аутентификации пользователей, и реализация механизма интеграции существующих приложений и всех компонент подсистемы безопасности.
Несмотря на существующие международные стандарты, определяющие функционирование системы PKI и способствующие ее взаимодействию с различными средствами защиты инфор мации, к сожалению, не каждое средство информационной защиты, даже если его производи тель декларирует соответствие стандартам, может работать с любой системой PKI. В нашей стране только начинают появляться компании, предоставляющие услуги по анализу, проектированию и разработке инфраструктуры открытых ключей. Поскольку при возрастаю щих масштабах ведомственных и корпоративных сетей VPN - продукты не смогут работать без PKI, только у разработчиков и поставщиков и VPN есть опыт работы в этой области.

Лицензии, сертификаты …

Корпоративную систему защиты информации должны осуществлять назначенные конкрет ные разработчик и поставщик, поскольку требуется именно комплексное решение проблемы, вместе с тем предмет корпоративной (часто чрезвычайно коммерчески дорогостоящей или су губо конфиденциальной) информации достаточно деликатен, то выбор разработчика и по ставщика должен определяться следующими критериями:

- наличие у разработчика соответствующих лицензий и сертификатов на осуществление такого рода деятельности;
- государственная сертифицированность применяемых разработчиком продуктов и ре шений соответствующими органами того государства, на территории которого создаются такие системы;
- положительный опыт разработчика в создании именно комплексных масштабных ре шений, начиная от разработки "политики…", продолжая непосредственным созданием системы защиты информации, и заканчивая поддержкой и непрерывным последующим мониторингом функционирования и использования системы;
- доверие к разработчику, основывающееся на его репутации в деловом мире, особенно в среде непосредственных пользователей предыдущих реализаций проектов разработчика.

Руководство, разработчики и персонал компании ЭЛВИС+ в полной мере обладают всеми вышеперечисленными способностями и качествами, чему примером наши успешные реализа ции проектов в ряде государственных и коммерческих организаций, в том числе относящихся к топливно-энергетическому комплексу, таких как ОАО "ЛУКОЙЛ", РАО "ЕЭС России" и т.д.