"Галереи IT-проектов"

«Сетевой журнал» №2 2002
ведущая рубрики Мария Суханова

Очередной выпуск нашей "Галереи IT-проектов" посвящен защите информации. Свои решения предложенной редакцией "Сетевого журнала" задачи обеспечения информационной безопасности предлагают четыре фирмы: "АйТи", "Инфотел", ОБИНКО и ЭЛВИС+. Сама же задача такова

Торговая фирма с распределенной структурой - четыре магазина, два склада и др. (см. схему) - испытывает серьезные проблемы с безопасностью данных.

Плохо защищены данные и транзакции, передаваемые между отделениями, электронная почта (имелись случаи несанкционированного чтения корреспонденции), информация, хранящаяся в базах клиентов, договоров и в базах, используемых программой "1С: Бухгалтерия" (здесь также зарегистрированы случаи несанкционированного доступа, в том числе и приводившие к нарушению целостности баз).

Контроль доступа и обнаружение вторжений в корпоративную сеть извне практически отсутствуют, при этом персонал, ответственный за информационную безопасность, не обладает достаточной квалификацией, чтобы идентифицировать вторжения.Особо отмечается высокая уязвимость Web-сервера.

Кроме проблем, есть пожелания: обеспечить удаленный защищенный доступ к ресурсам сети для мобильного персонала (менеджеров по закупкам и продажам, экспедиторов), а также сохранение единого рабочего окружения и настроек для сотрудников, имеющих по несколько рабочих мест в разных отделениях фирмы.Задачи проекта представляются заказчику следующими:
1. Проанализировать компьютерную сеть фирмы на предмет уязвимых мест.
2. Определить политику безопасности фирмы в отношении информационной системы и выработать рекомендации по административным мерам и другим средствам, не связанным с информационными технологиями.
3. Обеспечить защиту корпоративной сети от вторжений извне.
4. Обеспечить внутреннее разграничение доступа к конфиденциальной информации (финансовые данные, базы клиентов, договоров) и контроль безопасности наиболее важных узлов внутренней сети.
5. Организовать защиту информации, передаваемой через интернет в филиалы.
6. Организовать защиту интернет-сервера компании, желательно с возможностью отражения DoS-атак, а также вторжений с помощью "троянских коней", подбора паролей и др.
7. Обеспечить сохранение рабочих окружений сотрудников вне зависимости от их физического местонахождения и используемого канала связи.
8. Упростить и частично автоматизировать плановое администрирование системы защиты информации. Обеспечить централизованное управление устройствами системы

безопасности. Обеспечить конфиденциальность системных паролей при настройке и управлении серверами и сетевыми устройствами. 9. Обеспечить надежность и отказоустойчивость систем безопасности, а также защиту самих средств защиты.

Построенная система защиты должна удовлетворять требованиям масштабируемости в несколько раз от имеющегося числа рабочих мест, интеграциис существующими программными платформами и минимизации необходимых затрат, особенно связанных с обслуживанием.

Структура распределенной сети торговой фирмы показана на схеме (см. внизу статьи), там же перечислено основное оборудование и ПО, установленное в каждом из подразделений. Фирма работает с учетной системой "1С:Бухгалтерия" 7.5 (версия "клиент-сервер") и ведет также базы клиентов и договоров с помощью СУБД MS SQL Server 7.0 (клиент - MS Access 97). Операционные системы - Windows NT 4.0, на некоторых рабочих станциях также Windows 95; Netware 3.0 для файл-серверов, Linux для интернет-сервисов (кроме Web-сервера, который работает под управлением Windows 98).

Локальная сеть центрального офиса сегментирована с помощью коммутатора 3Com SuperStack II Switch 1100, а сегменты подключены к концентраторам 3Com OfficeConnect Ethernet Hubs; кабель - витая пара 5 категории. Сети всех торговых точек, сервисного подразделения и склада N1 реализованы на базе простых концентраторов и витой пары 3 категории, склада N2 - на базе тонкого коаксиального кабеля.

Подробности можно узнать на нашем сайте, но они не очень существенны. Во всех предложенных решениях прослеживается мысль о том, что выбор средств защиты определяется в первую очередь не имеющимся оборудованием или ПО и даже не структурой сети, а характером информации, которая в этой сети циркулирует. При этом, может быть, даже в большей степени, чем объективные параметры информации, важно субъективное отношение к ней владельца: чем выше он ценит хранящиеся и передаваемые данные, тем более серьезную защиту просит установить.

С другой стороны, авторы всех решений считают необходимым определенный минимальный набор защитных средств. Это антивирусное ПО (в задаче оно не упоминалось - видимо, антивирусная защита в фирме есть, и руководство считает ее достаточной, - но все же роль антивирусов подчеркивается во всех решениях), межсетевые экраны в местах подключения к интернету, шифрование данных, передаваемых по открытым каналам, разграничение доступа между пользователями корпоративной сети. Общей была также рекомендация по возможности модернизировать локальные сети, заменив концентраторы коммутаторами, и основную операционную систему, поскольку средства защиты в Windows 2000/XP значительно усовершенствованы по сравнению с NT.

И последнее, на что хотелось бы обратить внимание, - это в разных формах представленное в решениях соображение о том, что работа над системами безопасности требует большей активности со стороны заказчика, чем обычные проекты. Одни обязательные этапы интегратор при всем желании не смог бы взять на себя, другие клиенты сами обычно не готовы кому бы то ни было передоверить. Сказанное относится и к обслуживанию средств защиты - ряд операций с ними нельзя поручить никому постороннему. И здесь возникает проблема недостаточно квалифицированного персонала. Предложения по ее поводу различаются - кто-то рекомендует отказаться от слишком

сложных средств защиты, кому-то представляется более правильным найти или подготовить нужных специалистов. Решить это, конечно, тоже должен сам заказчик.

ЭЛВИС+:
объективность плюс конфиденциальность

Компания ЭЛВИС+ - системный интегратор, специализирующийся в области систем информационной безопасности, и разработчик серии программных продуктов ЗАСТАВА для сетевой защиты. Имеет лицензию Гостехкомиссии при Президенте РФ на деятельность в области защиты информации и лицензию ФСБ на работу со сведениями, составляющими государственную тайну, аккредитована ГТК для проведения аттестации систем информационной безопасности. Торговая марка Застава зарегистрирована в 1997 году. Все ПО Застава сертифицировано ГТК, а VPN-продукты этой марки содержат лицензированную технологию TrustWorks Systems (www.trustworks.com), удостоенную награды как технология нового тысячелетия (Technology Innovation for New Millennium Award) на Всемирном экономическом форуме в Давосе в январе 2000 года.

В ходе реализации проектов компания создала типовые решения по защите информационных ресурсов в распределенных сетях и выработала концепцию комплексного системного подхода к решению проблем информационной безопасности, которую в настоящее время применяет и продолжает развивать. Большое внимание она уделяет и вопросам правового обеспечения защиты информации.

У ЭЛВИС+ много проектов для корпораций, имеющих либо представительства в разных точках страны и даже земного шара, либо сотрудников, перемещающихся по всему миру и отовсюду подключающихся к корпоративной сети, либо и то и другое. Для связи при этом используются публичные сети - интернет и различные телефонные линии: стационарные, мобильные, подключение из гостиниц. Так что описанная в задаче торговая фирма, с точки зрения ЭЛВИС+, представляет собой довольно типичный случай компании с распределенной сетью.

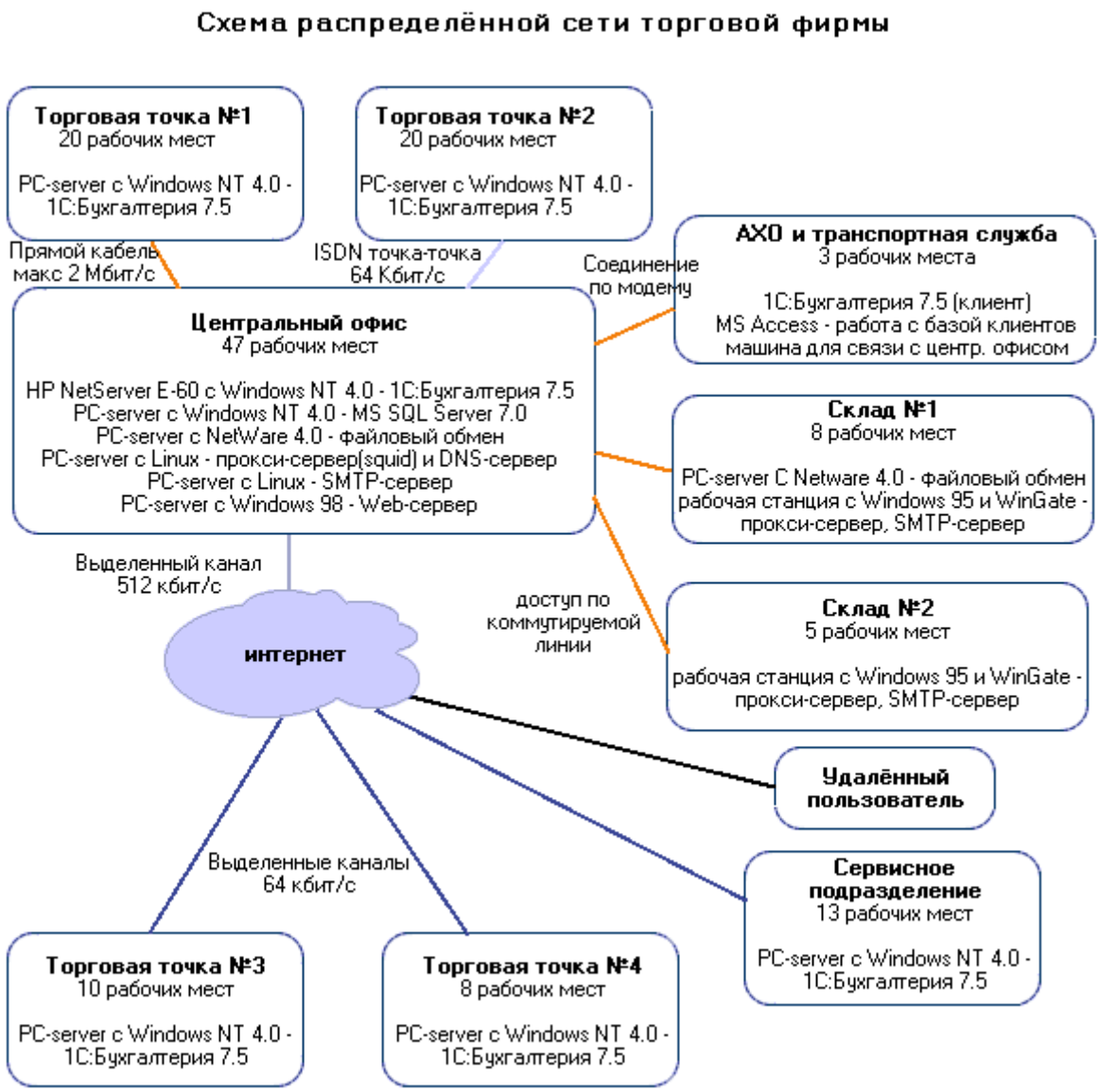

Рис. Схема распределенной сети торговой фирмы

Комплексное обследование

Работу над системой защиты для нашей торговой фирмы специалисты ЭЛВИС+ рекомендуют начать с комплексного обследования фирмы и написания проекта. Стоимость обследования определяется исходя из объема трудозатрат; для нашей торговой фирмы он ориентировочно составит около трех человеко-месяцев. Продолжительность обследования будет зависеть от пожеланий заказчика, поскольку если это нужно сделать быстро, ЭЛВИС+ может сформировать несколько бригад сотрудников, которые будут параллельно обследовать все точки распределенной сети и т. д.

Обследованию подлежат организационная структура, нормативно-распорядительная документация и сеть. По каждому из этих трех направлений ЭЛВИС+ подготавливает свои рекомендации.

При обследовании организационной структуры предприятия представители ЭЛВИС+ изучают документы, определяющие его юридический статус, структуру подразделений, схему руководства и т. п. Рекомендации здесь могут касаться таких вопросов, как,

например, разделение полномочий по защите между IT-отделом и службой безопасности (кстати, весьма болезненная проблема во многих фирмах).

Вторым направлением обследования является анализ нормативно-распорядительной документации, относящейся к защите информации, - если, конечно, такие распоряжения издавались. Рекомендации представляют собой список документов, которые необходимо разработать. В дальнейшем ЭЛВИС+ может оказать заказчику и помощь в составлении этих документов.

Наиболее важны приказы, констатирующие, что такая-то часть информации принадлежит фирме и является ее коммерческой, служебной или какой-то иной тайной, а также перечни составляющих тайну ресурсов. Ресурсы должны быть расклассифицированы по степени секретности - скажем, на особоважные, просто важные и т. д. Здесь возможны консультации со стороны ЭЛВИС+ по поводу статуса информации - целесообразно ли объявлять тот или иной ресурс составляющим тайну? Разумеется, компания всегда гарантирует сохранность информации клиента, и не было случая, чтобы она не выполнила своих обязательств.

Обследование сети носит уже более технический характер. Оно начинается с построения информационной модели предприятия, отображающей структуру сети и процедуры, посредством которых создается, циркулирует, обрабатывается и хранится информация. Затем фиксируется состояние сети и определяются точки, где возможны атаки, попытки несанкционированного доступа и т. д. Если заказчик уже имеет технические средства защиты, ЭЛВИС+ может проверить их эффективность путем активного аудита, т. е. имитируя (естественно, в заранее оговоренных рамках) действия недоброжелателя.

Почти весь нижеследующий материал посвящен рекомендациям, относящимся к сети.

Межсетевые экраны

Построение системы защиты для торговой фирмы можно начать с межсетевых экранов. Они позволят решить большинство проблем взаимодействия с внешними сетями и функционирования Web-сайта, а также контролировать доступ сотрудников к ресурсам интернета, которыми многие пользуются в, скажем так, неслужебных целях.

Система межсетевого экранирования допускает построение из нескольких "эшелонов". В качестве самого первого допустимо использовать списки доступа на маршрутизаторах - уже они дадут некоторую минимальную защиту. Затем специалисты ЭЛВИС+ рекомендуют установить в центральном офисе мощный полнофункциональный межсетевой экран, позволяющий не только отделить внутреннюю сеть от внешней, но и выделить буферную зону для обмена информацией между этими сетями; в такой зоне - ее называют "демилитаризованной" - стандартно размещается Web-сайт. Благодаря ее наличию внешние пользователи не попадут в корпоративную сеть, а будут по заданным правилам безопасности направлены через межсетевой экран на Web-сервер и к другим сервисам.

Межсетевой экран способен противодействовать очень многим типам хакерских атак. Даже самое простое действие - разрешить доступ к Web-серверу только по протоколу HTTP - предотвращает огромное число попыток несанкционированного доступа, а экран Firewall-1 компании CheckPoint позволяет отражать в том числе и DoS-атаки. ЭЛВИС+

выпускает и собственный экран серии ЗАСТАВА, но для данной задачи специалисты компании скорее рекомендовали бы все-таки Firewall-1 или брандмауэр производства Cisco, поскольку на их базе можно обеспечить расширенное протоколирование с контролем действий пользователей и анализом атак извне. Оно будет третьим эшелоном защиты.

Компания ISS (Internet Security Systems), предлагающая полный спектр продуктов для анализа уязвимости и обнаружения вторжений, выпускает специальный модуль к Firewall-1, который устанавливается в центре управления информационной безопасностью (о нем еще будет речь впереди). Этот модуль взаимодействует с межсетевым экраном, получая от него статистику и формируя стандартные отчеты, позволяющие узнать о загрузке соединения с интернетом, о попытках атак, о том, насколько эффективно те или иные сотрудники фирмы используют интернет, и т. п. Он также может оперативно реагировать на атаки и периодически проверять защищенность, имитируя атаку.

Что касается экрана ЗАСТАВА, то у него меньше функций, но зато он сертифицирован Гостехкомиссией при Президенте РФ на отсутствие недекларированных возможностей, что позволяет использовать его в организациях с высокими требованиями к безопасности, и ЭЛВИС+ поставляет его главным образом в государственные учреждения.

VPN

Перейдем теперь к другим офисам, имеющим выход в интернет. ЭЛВИС+ рекомендует, чтобы все подразделения осуществляли доступ к интернету централизованно, через главный офис. Добиться этого позволит виртуальная частная сеть - VPN, и в данном случае ЭЛВИС+ рекомендует семейство VPN-продуктов ЗАСТАВА собственной разработки.

Для организации VPN нужно установить программу "ЗАСТАВА-Сервер" на коммуникационных серверах удаленных офисов, через которые происходит обмен информацией. В центральном офисе на той же машине, что и Firewall-1, устанавливается "ЗАСТАВА-Офис". В результате мы получаем защищенный канал непосредственно до межсетевого экрана на выходе в интернет.

Поскольку технология VPN основана на стандартном протоколе IPSec, VPN-продукты совместимы между собой: например, с продуктом "ЗАСТАВА-Сервер" для Windows NT вполне может работать клиентская программа IPSec 9000 производства Hewlett-Packard, предназначенная для ОС HP-UX.

Последняя версия ЗАСТАВЫ - 3.3 - выпускается в вариантах для SUN Solaris 7 и 8, а также Windows 98, NT и 2000. Вариант для Windows 95 не распространяется, однако существует и может быть предоставлен по запросу, так что с ЗАСТАВОЙ для складов (если там почему-либо обязательно нужно сохранить Windows 95) проблем не возникнет. Но ЭЛВИС+, конечно, рекомендует обновить операционную систему, заменив ее на более современную и безопасную.

В ЗАСТАВЕ 3.3 появилось важное нововведение - центр управления средствами защиты, позволяющий одному-единственному системному администратору со своей консоли настраивать и конфигурировать средства защиты во всей распределенной VPN-сети. Соответствующий продукт произведен компанией TrustWorks Systems и называется

Trusted Global Security Manager. Он способен управлять всеми агентами VPN-продуктов ЗАСТАВА (т. е. программами "ЗАСТАВА-Клиент", "ЗАСТАВА-Сервер" и "ЗАСТАВА-Офис") независимо от платформы. Trusted Global Security Manager устанавливается на отдельный компьютер с Windows 2000, который должен быть достаточно мощным и иметь средства обеспечения отказоустойчивости (запасной блок питания, UPS, второй жесткий диск и т. д.), чтобы центр управления был постоянно наготове.

Еще одна интересная особенность версии 3.3 - наличие во всех агентах встроенного минимального набора функций межсетевого экрана. Поэтому если в каких-то точках окажется неудобно работать с интернетом через VPN и центральный офис, в них можно будет пользоваться прежним доступом, но уже в защищенном режиме. Впрочем, ЭЛВИС+ рекомендует такой вариант только как временный.

Дополнительно в состав VPN-продуктов ЗАСТАВА могут входить средства гарантированной идентификации пользователя. Для идентификации можно использовать дискеты, смарт-карты, USB-ключи, но самый надежный вариант - системы биометрического распознавания.

Разграничение доступа внутри сети

При построении системы защиты необходимо разграничить права пользователей на доступ к информационным ресурсам. Наша торговая фирма, как считают специалисты ЭЛВИС+, могла бы здесь пойти двумя путями: либо сегментировать сеть, либо двигаться от применяемых технологий.

По-видимому, фирме стоило бы модернизировать свои безнадежно устаревшие локальные сети, установить коммутаторы, поддерживающие VLAN, и сегментировать сеть на основе виртуальных локальных сетей. Однако можно разделить информационные потоки и с помощью технологии VPN (целесообразно ли это, выясняется при обследовании): на все рабочие станции устанавливается "ЗАСТАВА-Клиент", на серверы -"ЗАСТАВА-Сервер", и трафик каждого пользователя оказывается столь же недоступным для остальных, как и в случае применения коммутаторов. Проекты, где ЗАСТАВА установлена на каждой машине, действительно существуют; они разрабатывались для организаций с очень серьезными требованиями к безопасности. Возможен и смешанный вариант: в зоне сети, где циркулирует наиболее важная информация, используется VPN, в остальной сети - VLAN.

Под движением "от технологии" имеется в виду следующее. Во многие прикладные программы встроены очень неплохие функции обеспечения безопасности, которыми, разумеется, нужно пользоваться. Для этого специалисты ЭЛВИС+ на этапе аудита оценивают, насколько хорошо встроенные функции используемых программных продуктов способны обеспечивать конфиденциальность, целостность, доступность, разграничение прав пользователей и т. п., и если соответствующие средства достаточно развиты, дают рекомендации по их применению.

Например, СУБД Oracle имеет режим защищенного обмена информацией - естественно, это нужно использовать. Протоколирование, которое есть во многих СУБД, также должно быть использовано, чтобы случаи несанкционированного доступа хотя бы регистрировались - тогда по ним можно провести служебное расследование. Если же

аудит показывает, что встроенных защитных функций недостаточно, их можно усилить с помощью специальных дополнительных средств.

Для компьютеров с Windows 95/98 при невозможности переустановить на них ОС необходимы специальные средства защиты от несанкционированного доступа. Если же замена операционной системы допустима, ее лучше произвести.

Требование о сохранении рабочего окружения пользователей независимо от их местонахождения можно выполнить просто с помощью встроенных средств Windows NT/2000/XP. Для Windows 95/98 понадобятся дополнительные средства авторизации.

Защита от вредоносных программ

Для защиты от вирусов, "троянских коней" и т. п. необходимо в первую очередь ввести меры предосторожности при работе с интернетом и электронной почтой: именно они на настоящий момент являются главными каналами распространения вредоносных программ. Следует отключить Java-апплеты и приложения ActiveX в браузерах, автоматическую распаковку вложений в почтовых программах и т. д., о чем руководство должно издать соответствующее распоряжение. Конечно, это будет ограничение, но оно избавит фирму от многих неприятностей.

Если к административным мерам прибегать не хочется, то рекомендованный выше пакет Firewall-1 может сопрягаться со специализированным антивирусным шлюзом. Эта программа устанавливается на отдельную машину и фильтрует как почтовый трафик (SMTP), так и другие интернет-трафики (протоколы HTTP и FTP).

Но антивирусное ПО, разумеется, тоже нужно, поскольку кроме двух названных главных каналов - интернета и электронной почты - вирусы могут распространяться и по другим. С точки зрения функциональности имеющиеся на рынке антивирусы практически эквивалентны, так что выбор зависит от того, какой пакет лучше подходит к данной информационной системе: не вызывает значительного замедления работы сети, не конфликтует с имеющимися программами и т. д. Желательно использовать продукт, допускающий централизованное администрирование; пользователи не должны иметь возможности менять настройку антивирусной программы на своей машине.

Надежность защиты

Каким образом обеспечивать надежность работы системы безопасности? Это зависит от степени критичности сервисов, предоставляемых фирмой. В обычном случае специалисты ЭЛВИС+ считают, что для центра управления защитой достаточно просто качественной аппаратной платформы со стандартным набором средств повышения отказоустойчивости, а если требования очень высокие, рекомендуют использовать резервный сервер в "холодном" или "горячем" режиме. Желательно также, чтобы этот центр находился в отдельном помещении, в котором целесообразно поместить также межсетевой экран и другие средства защиты информации и управления информационной безопасностью; туда будет иметь доступ администратор по безопасности.

Следует предусмотреть систему резервирования важной информации, относящейся к защите, скажем паролей, чтобы ее легко было восстановить в случае утраты. Очень серьезным организациям, возможно, следует рассмотреть вопрос о режимном помещении для серверов защиты.

Жизнь в безопасности

Проекты систем безопасности, подготовленные ЭЛВИС+, всегда разбиваются на этапы в зависимости от срочности, так что заказчик может решить сначала самые неотложные проблемы защиты, а затем постепенно усовершенствовать защиту по мере того, как у него будет появляться возможность.

Каждый этап сдается отдельно, при этом проводятся приемосдаточные испытания по согласованной методике. Затем внедренные на данном этапе средства защиты поступают в опытную эксплуатацию, а через положенное время переводятся в промышленную.

Главная цель опытной эксплуатации - помочь сотрудникам фирмы или организации адаптироваться к новым условиям работы. ЭЛВИС+ организует обучение специалистов заказчика, но его обычно недостаточно - необходима практика.

По наблюдениям специалистов ЭЛВИС+, рядовые сотрудники поначалу обычно скорее недовольны внедрением системы безопасности - просто потому, что они не любят никаких изменений. И чтобы это внедрение было успешным, необходима очень высокая активность руководства. Собственно, инициатива также всегда исходит в первую очередь именно от него.

После того как люди освоятся с защитой, их отрицательная реакция исчезает. И нельзя не признать, что, узнав о возможности мониторинга путешествий по интернету, многие начинают проводить меньше времени на посторонних сайтах и больше заниматься своим делом.