Дипломная работа Тема: Анализ проблем информационной безопасности в компьютерной сети организации, подключённой к сети интернет

Выполнил Столяров

Рук. дипломной работы: Ахмедов А.Ш

О В данной дипломной проекте объектом исследования является локальная вычислительная сеть предприятия. Предметом исследования данного дипломного проекта являются структура и функционирование локальной компьютерной сети. Цель работы состоит в анализе проблем информационной безопасности в сети предприятия, подключенной к сети Интернет. Для достижения указанной цели необходимо решить следующие задачи: О -провести анализ угроз информационной безопасности; О -предложить метод и способ защиты существующей локальной компьютерной сети.

Актуальность вопросов информационной безопасности в сети предприятия определяется следующими причинами: О постоянное развитие и усложнение оборудования и приложений, используемых в корпоративной сети; О наличие технологических недостатков, обусловленных проблемами защиты в компьютерных технологиях; О недостатки конфигурации, реализации и использование технологии защиты, результатом чего может оказаться появление проблем защиты; О ошибки и недостатки в организации политики защиты, что может привести к уязвимости даже самую лучшую технологию сетевой защиты

Основными факторами, способствующими повышению уязвимости информации, являются:

-резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;

-сосредоточение в единых базах данных информации различного назначения;

-резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам информационной системы и находящимся в ней данных;

-усложнение режимов функционирования технических средств вы-числительных систем: широкое внедрение многопрограммного режима; автоматизация межмашинного обмена информацией, в том числе и на больших расстояниях.

Методами и способами защиты информации от несанкционированного доступа являются:
-реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием документам;
-ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;
-разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
-регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
-учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
-резервирование технических средств, дублирование массивов и носителей информации;
-использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
-использование защищенных каналов связи;
-размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
-организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;
-предотвращение внедрения в информационные системы вредоносных и программных закладок.

Средним и крупным предприятиямсвойственны повышенные требования к безопасности. При широком использовании сети Интернет возникает необходимость решения проблемы защиты информации и локальной сети в целом. Решение заключается в разделении локальной сети и публичных серверов на отдельные части - создание DMZ, доступ к которой осуществляется только по заранее заданным правилам межсетевого экрана.

В результате анализа существующих средств защиты сетей в качестве межсетевого экрана было выбрано следующее устройство: О межсетевой экран Zyxel ZywallUSG 1000 Производительный центр безопасности О это компактный скоростной шлюз доступа нового поколения, обеспечивающий комплексное решение задач сетевой безопасности и управления трафиком, включая потоковый антивирус, обнаружение и предотвращение вторжений, защиту от спама, контроль полосы пропускания для разнообразных объектов сети и безопасность удаленных подключений при помощи виртуальных частных сетей. Устройство имеет интуитивный пользовательский интерфейс с перекрестной системой навигации, встроенным справочником и графическим мониторингом состояния. Объектно-ориентированная модель управления позволяет максимально оптимизировать настройку даже в сложных сетях.

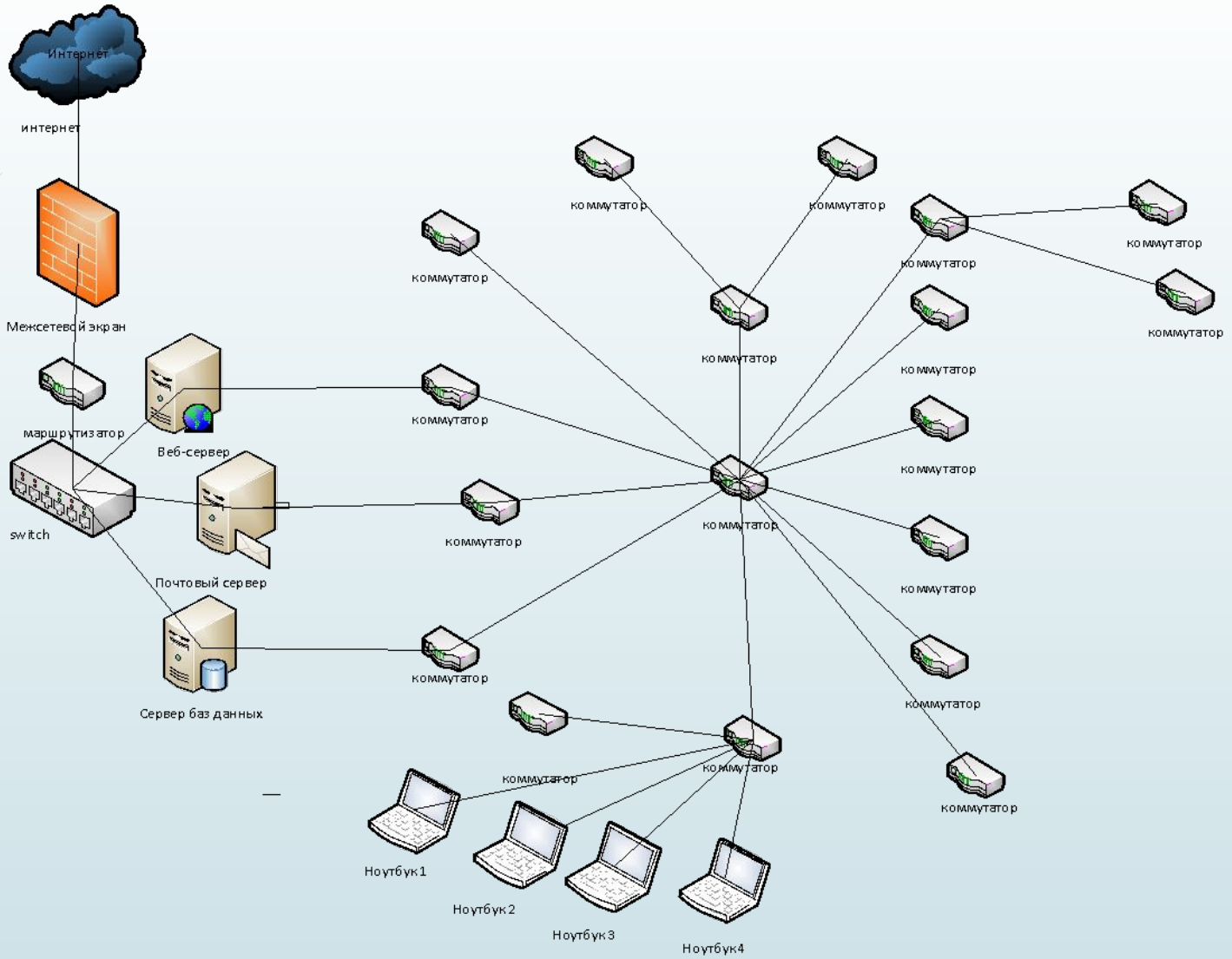

Схема ЛВС предприятия с подключённым межсетевым экраном

Спасибо за внимание