**МДК 01.01.Т2 Безопасность и управление доступом в ИС**

«Технологическая модель подсистемы информационной безопасности»

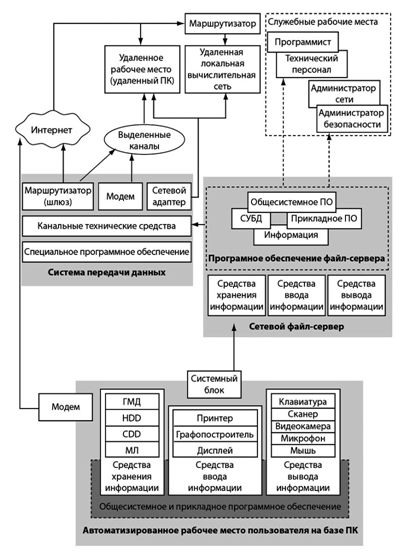
Современные распределенные корпорации, имеющие подразделения на разных континентах, имеют сложную техническую, инженерную и информационную инфраструктуру. Создание информационной сети такой корпорации и её эффективная защита является чрезвычайно сложной концептуальной и технологической задачей.

Первоначальное решение, характерное для последнего десятилетия прошлого века, использовать для формирования сети телефонные линии быстро привело к нагромождению коммуникаций и к невозможности эффективной защиты. Последующее создание и сопровождение собственных корпоративных сетей для обеспечения информационного обмена данными на базе таких линий связи стало обходиться в миллионы долларов.

Быстрое развитие технологий Internet, образование, рост и развитие "всемирной паутины" позволили создать достаточно дешевые и надежные коммуникации. Однако техническая надежность связи вовсе не означала безопасности корпоративных сетей, имеющих выходы в Интернет. Общие принципы построения Интернет и его использование как общедоступной сети с публичными сервисами привели к тому, что стало очень трудно обеспечить надежную защиту от проникновения в корпоративные и государственные сети, построенные на базе протоколов TCP/IP и Internet -приложений — Web, FTP, e-mail и т.д.

Целевое назначение любой корпоративной информационной системы состоит в обеспечении пользователей необходимой информацией в режиме "On Line" и адекватном информационном сопровождении деятельности предприятия.

Базисом КИС является общесистемное программное обеспечение, которое включает операционную систему и программные оболочки, программы общего и прикладного назначения: автоматизированные рабочие места (АРМ) и Web-сервисы общего и специального назначения, СУБД и управление интегрированными вычислительными и мультимедийными приложениями, а также доступом в локальные и внешние сети.



**Рис. 1.** Схема корпоративной информационной системы, включающей локальные сети и выход в Internet

Физически нижний уровень КИС базируется на серверах, рабочих станциях, персональных компьютерах различного назначения и коммуникационных устройствах, а также на программном обеспечении, реализующем работу перечисленных устройств. В связи с этим подсистема ИБ начинается с защиты именно этого программно-аппаратного оборудования. С этой целью можно использовать известные защитные средства операционных систем, антивирусные пакеты, средства и устройства аутентификации пользователя, средства криптографической защиты паролей и данных прикладного уровня. Все эти средства образуют базу для реализации первого уровня технологической модели подсистемы ИБ.



**Рис. 2.**Четырехуровневая технологическая модель подсистемы информационной безопасности

Второй физический уровень КИС — рабочие станции, серверы и персональные компьютеры объединятся в локальные сети, которые организуют внутреннее Intranet-пространство предприятия и могут быть иметь выходы во внешнее Internet-пространство.

В этом случае речь идет о средствах информационной защиты (СЗИ) второго уровня — уровня защиты локальных сетей, который обычно включает:

* средства безопасности сетевых ОС;
* средства аутентификации пользователей (User Authentication Facilities — UAF);
* средства физического и программного разграничения доступа к распределенным и разделяемым информационным ресурсам;
* средства защиты домена локальной сети (Local Area Network Domain — LAND);
* средства промежуточного доступа (Proxy Server) и межсетевые экраны (Firewall);
* средства организации виртуальных локальных подсетей (Virtual Local Area Network — VLAN);
* средства обнаружения атаки и уязвимостей в системе защиты локальных сетей.

Следующий уровень реализации КИС — объединение нескольких локальных сетей географически распределенного предприятия в общую корпоративную Intranet-сеть через открытую сеть на базе современных технологий поддержки и сопровождения таких сетей (Quality of Service — QoS) с использованием открытой среды Internet в качестве коммутационной среды.

В этом случае на третьем уровне защиты КИС используются технологии защищенных виртуальных сетей (Virtual Private Networks — VPN). VPN-технологии часто интегрируются со средствами первого и второго уровней. Такой защищенный VPN-канал может простираться не только до маршрутизаторов доступа и пограничных Firewall'лов, но и до серверов и рабочих станций локальной сети.

Четвертый уровень защиты КИС — организация защищенного межкорпоративного обмена в среде электронного бизнеса (eBusiness). Методологической и технологической основой такой защиты являются методы и технологии управления публичными ключами и сертификатами криптографической защиты (Public Key Infrastructure — PKI). Суть этих технологий состоит в реализации двух глобальных функций: генерации и корректном распространении ключей и сертификатов и отслеживании их жизненного цикла. Базой для реализации средств защиты будут электронная цифровая подпись (Electronic Digital Signature — EDS) и VPN-технологии.

Отметим, что два нижних уровня защиты являются достаточно традиционными, так как они предназначены для обеспечения безопасности конкретной физически реализованной КИС. Верхние два уровня относятся к обеспечению безопасности передачи данных и электронного бизнеса, который осуществляется уже не в физическом, а в виртуальном пространстве, при этом VPN-технологии обеспечивают защищенный обмен данными в межкорпоративном пространстве, а PKI-технологии обеспечивают VPN-устройства ключами и сертификатами. В настоящее время на рынке имеется достаточное число технических и программных решений для защиты данных, информации, систем и сетей. Ниже рассмотрены некоторые базовые технологии на примере криптографической защиты данных, технологий межсетевых экранов, защищенных VPN-каналов связи, антивирусных и биометрических методов.