

УДК 004

ЗАЩИТА ЛОКАЛЬНЫХ СЕТЕЙ

**Степанова Ю.Н., студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В., к.э.н., доцент
ФГБОУ ВО Ульяновский ГАУ**

Ключевые слова: защита, информация, локальные сети, пользователь, интернет.

Статья посвящена решению задачи повышения защиты информации (передачи данных), которая возникает при разработке и развертывании локальной компьютерной сети.

Актуальность темы статьи обосновывается тем, что она направлена на разрешение объективного противоречия, сложившегося в настоящее время, между возрастающей потребностью увеличения числа локальных сетей и их пользователей, с одной стороны, и ограниченными возможностями каналов связи обеспечить высокую пропускную способность, информационную безопасность и низкую стоимость, с другой стороны.

Защита информации — это деятельность по предотвращению утечки, хищения, утраты, подделки, несанкционированных воздействий на защищаемую информацию. Так как утрата информации может происходить по техническим и неумышленным причинам, под это определение попадает также деятельность, связанная с повышением надежности сервера из-за отказов или сбоев в работе винчестеров.

С установкой локальной сети и подключением организации к Internet проблема безопасности возникает на 2-ух уровнях:

- Масштаба предприятия - защита от различного рода вторжений и атак, а также регулировка доступа пользователей к ресурсам в Internet, например, запрет посещения определенных групп сайтов.

- Пользователя - разграничение доступа пользователей к ресурсам внутри сети, политика безопасности и защита для каждого отдельного рабочего места.

Существующие и наиболее распространенные средства защиты локальных сетей на сегодняшний день можно разбить на следующие группы:

- Средства защиты, перекрывающие доступ несанкционированным пакетам со стороны Интернет в локальную сеть, которая охраняется;

- Средства защиты доступа к системе со стороны потребителей ресурсов системы или пользователей, эксплуатирующих систему;
- Средства, оказывающие неоднородности в сети Интернет, возникают в системе, охраняемых и могут быть объектом атаки;
- Средства защиты данных и программных компонентов, используемых в системе.

Данные методы защиты также могут подойти, когда компьютер подключен к другому компьютеру напрямую, в этом методе не нужно использовать роутер.

Типичным представителем первой группы является Firewall, который структурно размещается на входе в систему и соединяющий локальную сеть с сетью Интернет.

Типы Firewall: Пакетные фильтры, Динамические пакетные фильтры, Прокси-агенты.

Функции, которые обеспечивает Firewall:

- Фильтрация пакетов,
- Трансляция сетевых адресов, которая заключается в том, что Firewall заменяет адрес IP внутреннего хоста на собственную, внешнюю, что делает внутренние адреса хостов локальной сети недоступны внешним хостам сети Интернет.
- Услуги прокси, которые заключаются в предоставлении соединения на прикладном уровне от имени внутреннего хоста, что позволяет использовать услугу прокси в качестве промежуточной памяти для данных, которыми обмениваются внешние хосты с хостами внутренними.

Кроме того, Firewall можно использовать для верификации пользователей, использующих для доступа внешние хосты. Дополнительным преимуществом, которую обеспечивает Firewall, является формирование туннеля, с помощью которого формируется защищенный канал. Это позволяет шифровать внутренний пакет в таком туннельном канале связи.

Для решения проблемы защиты информации основными средствами, используемыми для создания механизмов защиты принято считать:

Технические средства — электрические, электромеханические, электронные и др. типа устройства. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Технические средства подразделяются на:

- аппаратные — устройства, встраиваемые непосредственно в аппаратуру, или устройства, которые сопрягаются с аппаратурой локальных сетей по стандартному интерфейсу;

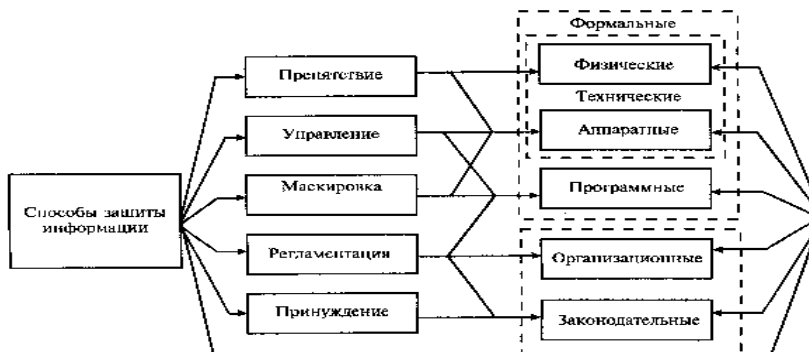


Рисунок 1 - Концепция защиты информации

- физические — реализуются в виде автономных устройств и систем.

В ходе развития концепции защиты информации специалисты пришли к выводу, что использование какого-либо одного из выше указанных способов защиты, не обеспечивает надежного сохранения информации. Необходим комплексный подход к использованию и развитию всех средств и способов защиты информации.

Библиографический список

1. Башлы, П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебник / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. - М.: РИОР, 2013. - 222с.
2. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш.- 2-е изд.- М.: РИОР: ИНФРА-М, 2014.- 256с.
3. Защита информации: учебное пособие / Жук А.П. [и др.]- М.: ИНФРА-М, 2013.- 392 с.

PROTECTION OF LOCAL NETWORKS

Stepanova Y.N.

Keywords: protection, information, local networks, user, Internet.

The article is devoted to the task of increasing the protection of information (data transfer), which occurs when developing and deploying a local computer network. The relevance of the topic of the article is justified by the fact that it is aimed at resolving the objective contradiction that has arisen at present between the growing need to increase the number of local networks and their users, on the one hand, and the limited capabilities of communication channels to provide high throughput, information security and low cost, on the other hand.