УДК 004

БЕЗОПАСНОСТЬ В ЛОКАЛЬНЫХ СЕТЯХ

Порфильева А.М.,студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В., к.э.н., доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *локальная сеть, обеспечение безопасности, информация, угрозы, методы защиты.*

В статье рассказывается о безопасности в локальной сети. О методах защиты локальной сети от внутренних и внешних угроз.

Локальная вычислительная сеть – это компьютерная сеть, охватывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт).[3]

Важно понимать, что безопасность локальной сети— это не продукт, который можно купить в магазине и быть уверенным в собственной защищенности. «Безопасность» — особое сочетание как технических, так и административных мер.

Согласно статистике потерь, которые несут организации от различных компьютерных преступлений, наибольшую долю занимают потери от преступлений, совершаемых собственными недобросовестными сотрудниками. Однако, в последнее время, наблюдается явная тенденция к увеличению потерь от внешних злоумышленников (рисунок 1). В любом случае, необходимо обеспечить защиту как от нелояльного персонала, так и от способных проникнуть в вашу сеть хакеров. Только комплексный подход к защите информации может внушить уверенность в ее безопасности.[2]

Существует несколько методов защиты локальной сети от внутренних и внешних угроз: парольная защита информации, ограничение доступа к информации, использование прокси-сервера, антивирусные системы, использование брандмауэра, контроль учётных записей и другие.

Для защиты циркулирующей в локальной сети информации также можно применить следующие криптографические методы: шифрование информации и электронную цифровую подпись (ЭЦП).

- Шифрование информации помогает защитить ее конфиденциальность, т.е. обеспечивает невозможность несанкционированного ознакомления с ней. Шифрование — это процесс

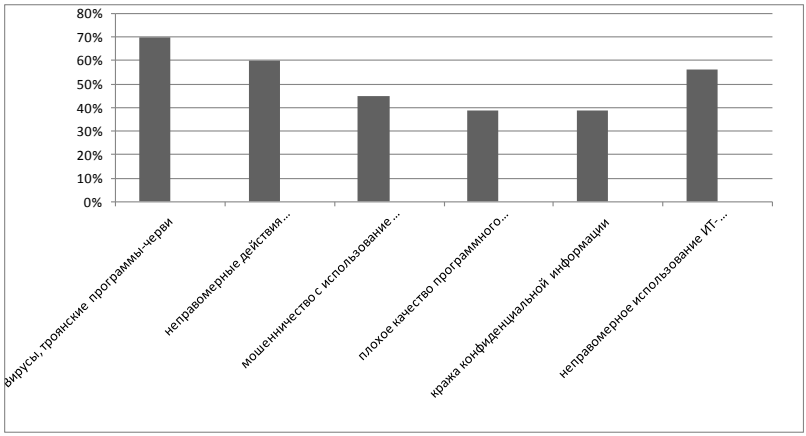

Рисунок 1.

преобразования открытой информации в закрытую, зашифрованную и наоборот. Это преобразование выполняется по строгим математическим алгоритмам; помимо собственно данных в преобразовании также участвует дополнительный элемент — «ключ». Ключ представляет собой уникальный элемент, позволяющий зашифровать информацию так, что получить открытую информацию из зашифрованной можно только определенному пользователю или группе пользователей.

- ЭЦП позволяет гарантировать целостность и авторство информации. Электронная цифровая подпись также использует криптографические ключи: секретный и открытый. Секретный ключ должен оставаться у его владельца, открытый же распространяется всем пользователям, желающим проверять ЭЦП владельца секретного ключа. Необходимо обеспечивать недоступность своего секретного ключа, иначе злоумышленник легко может подделать ЭЦП любого пользователя, получив доступ к его секретному ключу.[1]

Подводя итог, можно с уверенностью говорить о том, что вопрос информационной безопасности в локальных вычислительных сетях останется актуальным еще достаточно долгое время. Компьютерные сети, в силу своей специфики, не смогут нормально функционировать и развиваться, игнорируя проблемы защиты информации.

Библиографический список:

1. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы / В. Олифер, Н. Олифер . - Питер - Москва, 2013. - 944 с.
2. Чекмарев, Ю.В. Локальные вычислительные сети / Ю.В. Чекмарев. – Москва: ДМК Пресс, 2009. - 200 с.
3. Локальная вычислительная сеть [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/wiki

SECURITY IN LOCAL NETWORKS

Porfiljeva A.M.

Keywords: *local network, security, information, threats, methods of protection.*

The article discusses security in the local network. About methods of protection of the local network from internal and external threats.