МОДЕЛИ УГРОЗ ЛОКАЛЬНОЙ СЕТИ В УЧРЕЖДЕНИИ ОБРАЗОВАНИЯ

Силич С.С.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шевчук О.Г. – канд. тех. наук, доцент

Рассмотрены виды угроз, возникшие в компьютерных локальных сетях, их отличительные особенности. Предложены общие рекомендации по применению как программных, так и аппаратных способов устранения угроз.

Современные информационные системы имеют сложную структуру. Они содержат пользовательские приложения, работающие во взаимодействии с различными операционными системами, установленными на компьютерах, объединенных в локальную сеть, часто связанную тем или иным образом с сегментом глобальной сети. Обеспечение безопасности требует проведения целого комплекса мероприятий в соответствии с разработанной на предприятии политикой информационной безопасности [1].

Существует два возможных направления политики информационной безопасности:

1. Ограничительная политика, пользователь имеет право использовать любые ресурсы, кроме тех, доступ к которым ограничен или закрыт.

2. Нормативная политика, пользователь имеет право использовать только те ресурсы, которые ему явным образом выделены.

Информационная безопасность обеспечена в случае, если для любых информационных ресурсов в системе поддерживается определенный уровень конфиденциальности (невозможности несанкционированного получения какой-либо информации), целостности (невозможности несанкционированной либо случайной ее модификации) и доступности (возможности за разумное время получить требуемую информацию). При этом учитывается не только вероятность нарушения какого-либо из аспектов безопасности в результате умышленных либо неумышленных действий пользователей, но и вероятность выхода из строя каких-либо узлов информационной системы [2].

Многоуровневая защита информационной сети:

1. Внешний уровень определяет взаимодействие информационной системы организации с глобальными ресурсами и системами других организаций.

2. Сетевой уровень связан с доступом к информационным ресурсам внутри локальной сети организации. Безопасность информации на этом уровне обеспечивается средствами проверки подлинности пользователей и разграничением доступа к ресурсам локальной сети (аутентификация и авторизация).

3. Системный уровень связан, прежде всего, с управлением доступом к ресурсам ОС. На этом уровне происходит непосредственное взаимодействие с пользователями, запускаются приложения, и определяются «правила игры» между информационной системой и пользователем (задается либо изменяется конфигурация системы).

4. Уровень приложений связан с использованием прикладных ресурсов информационной системы. Поскольку именно приложения на содержательном уровне работают с пользовательскими данными, для них, нужны собственные механизмы обеспечения информационной безопасности.

При организации защиты от интернет-угроз важным является понятие периметра – укреплённой границы сети. Периметр может состоять из различных подсистем, как представленных различными аппаратными и программными средствами, так и объединёнными в единый программно-аппаратный комплекс. Такими подсистемами обычно являются:

- маршрутизаторы (routers);
- межсетевые экраны (брандмауэры, firewalls);
- прокси-серверы;
- системы обнаружения вторжений (IDS);
- средства создания виртуальных частных сетей (VPN);
- антивирусные средства;
- экранированные подсети

Таким образом, основным типом угроз является атака. Для её минимизации рекомендуется: применять прокси-сервера как единой точки выхода в сеть Интернета; на сервере с прокси сервером установку межсетевого экрана (программного или аппаратного); доступ к ресурсам сети через логин и пароль с ограничением на число попыток.

Список использованных источников:

1. Технологии Репликации [Электронный ресурс] – Режим доступа: https://techrepl.ru/uslugi/ddos.html