ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМ ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ

Т.В. Борботько

В современном обществе наблюдается устойчивая тенденция внедрения информационных технологий в различные сферы его жизнедеятельности. Это приводит к ряду положительных эффектов, таких как упрощение доступа населения к различным видам услуг, в промышленности – сведение к минимуму ошибок при реализации технологических процессов, для бизнеса – появление новых рынков сбыта и способов монетизации и т. д. Вместе с тем, доступность информационных систем различного назначения привлекает внимание к ним исследователей, в том числе тех, которые ориентированы на деструктивное вмешательство в процесс функционирования таких систем. Исходя из особенностей действия нарушителя, можно сформулировать следующие принципы.

Первый принцип – информированности. Построение эффективной системы защиты информации основано на понимании модели нарушителя. Это позволяет спланировать и подготовить ряд необходимых организационно-технических мероприятий по противодействию ему.

Второй принцип – многозональности. Любая информационная система содержит информационные ресурсы, критичность которых для обеспечения бизнес процессов в организации различна. Обнаружить и остановить кибератаку на периметре сети – чрезвычайно сложное мероприятие. Исходя из этого информационную сеть необходимо разделить на различные зоны, что позволит ее «замедлить» и выиграть время для ее обнаружения.

Третий принцип – восстанавливаемости. Одна из составляющих ущерба от кибератаки – это время простоя организации, которое может быть обусловлено, например, выводом из строя оборудования вследствие функционирования вредоносной программы.

Изложенные принципы противодействия кибератакам учитывают особенности их реализации и могут быть использованы при планировании соответствующих организационно-технических мероприятий.