УДК 316.776:351

В.Н. Федорченко, О.А. Берлизева

Харьковский национальный экономический университет, Харьков

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ

Угроза безопасности это возможность осуществления действия, направленного против объекта защиты, проявляемая в опасности искажений и потерь информации. Необходимо также учитывать, что источники угроз безопасности могут находиться как внутри предприятия - внутренние источники, так и вне ее – внешние источники. Такое деление оправдано потому, что для одной и той же угрозы (например, в случае кражи) методы отражения для внешних и внутренних источников будут разными. Все источники угроз безопасности информации можно разделить на три основные группы: угрозы, обусловленные действиями субъекта (антропогенные); угрозы, обусловленные техническими средствами (техногенные); угрозы, обусловленные стихийными источниками.

Первая группа, самая обширная, представляет наибольший интерес с точки зрения организации отражения угрозам данного типа, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия этим угрозам управляемы и напрямую зависят от воли организаторов защиты информации.

Субъекты, действия которых могут привести к нарушению безопасности и формации, могут быть как внешние так и внутренние.

Действия субъектов могут привести к ряду нежелательных последствий, среди которых можно выделить следующие: кража, подмена (модификация), уничтожение (разрушение), нарушение нормальной работы (прерывание), ошибки, перехват информации (несанкционированный).

Вторая группа содержит угрозы, менее прогнозируемые, напрямую зависящие от свойств техники и поэтому требующие особого внимания. Технические средства, содержащие потенциальные угрозы безопасности информации, также могут быть внутренними и внешними.

Последствиями применения таких технических средств, напрямую влияющими на безопасность информации, могут быть: нарушение нормальной работы, уничтожение (разрушение), модификация (изменение)

Третью группу составляют угрозы, которые совершенно не поддаются прогнозированию, и поэтому меры их отражения должны применяться всегда. Стихийные источники, составляющие потенциальные угрозы информационной безопасности как правило, являются внешними по отношению к рассматриваемому объекту и под ними понимаются, прежде всего, природные катаклизмы.

Даже первичный анализ приведенного перечня угроз безопасности информации показывает, что для обеспечения комплексной безопасности необходимо прикрытие как организационных, так и технических решений отражения.

Такой подход позволяет дифференцированно подойти к распределению материальных ресурсов, выделенных на обеспечение информационной безопасности. Наложение угроз безопасности информации на модель ИТ-преприятия позволяет в первом приближении оценить их опасность и методом исключения выделить наиболее актуальные для конкретного объекта защиты.

Список литературы

1. Биячуев Т.А. Безопасность корпоративных сетей / Т.А. Биячуев. – СПб: ГУ ИТМО, 2004. – 161 с.

2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – К.: DiaSoft, 2002. – 688 с.