УДК 004.7

Методики оценки рисков

Белова С.В.
Белорусский национальный технический университет

Абсолютная безопасность информационной системы не может быть достигнута никакими средствами. Всегда остается вероятность появления уязвимостей и проведения атак.

Мерой опасности атак является возможный ущерб. Ущерб – это негативное влияние на систему проведенной атакой. В качестве ущерба рассматриваются не столько потери на восстановление системы, сколько бизнес-потери, которые в результате нарушений понесло предприятие.

Вероятностная оценка величины возможного ущерба, который может понести предприятие в результате успешно проведенной атаки называется риском. Чем более уязвимой является существующая система безопасности, тем выше вероятность реализации атаки и, следовательно, тем выше значение риска.

Управление рисками – это системный анализ угроз, прогнозирование и оценка их последствий для предприятия и выбор контрмер, направленных на уменьшение возможного негативного воздействия нарушений на деятельность предприятия. Управление рисками обязательно включает оценку рисков. Существуют различные методики оценки рисков. Один из простейших методов состоит в умножении возможной величины потенциального ущерба на вероятность возникновения атаки. Чем больше полученное число, тем больше угроза системе.

Еще один способ оценки риска был предложен компанией Microsoft. Он получил название DREAD-методика — по первым буквам английских названий следующих категорий:

1) Потенциальный ущерб (Damage potential) — мера ущерба от успешной атаки.

2) Воспроизводимость (Reproducibility) — мера возможности реализации атаки.

3) Подверженность взлому (Exploitability) — мера усилий и квалификации, необходимых для атаки.

4) Круг пользователей, попадающих под удар (Affected users) — доля пользователей, работа которых нарушается из-за успешной атаки.

5) Вероятность обнаружения (Discoverability).

Суммарная DREAD-оценка равна арифметическому среднему всех оценок. После вычисления риска всех опасностей их сортируют в порядке убывания оценки, начиная с наибольшей.