ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

О.А. Вольская

На современном этапе на компьютерах, оснащенных новейшим программным обеспечением, процесс аутентификации сложен и используются длинные, путаные пароли и за системами следят самые квалифицированные администраторы — все равно остаются уязвимые места, т. к. человек, как правило, самое слабое звено в системе защиты.

Возможно, именно поэтому достаточно часто злоумышленники используют метод социального инжиниринга, основанный на использовании слабостей человеческого фактора. Целью этого метода является кража информации.

Таким образом, злоумышленник должен неплохо разбираться в психологии.

Выделяют три стадии подготовки такого рода атаки:

1. Определение точной цели, определение местоположения конечной цели. На данном этапе злоумышленник сначала пытается четко определить, за какого рода информацией он охотится, ведь если это ясно, то операция производится быстро: путем введения в заблуждение жертвы получается root и копируется необходимая информация;

2. Сбор информации об объекте обработки - это наиболее важный этап, во время которого похититель информации собирает сведения о характере жертвы, ее предпочтениях, привычках и уязвимых местах, чтобы свести время для получения информации к минимуму;

3. Разработка плана действий, моральная подготовка/тренировка. На данной ступени проводится просто колоссальная работа в области психологии: буквально каждое слово сопоставляется с психологической моделью изученной жертвы, необходимо просчитывать каждое слово, в зависимости от объекта, ведь люди разные и реакция на одно и то же слово у каждого разная.

Таким образом, следует обратить серьезное внимание на сложившуюся ситуацию и вести разработку систем защиты с учетом всего вышеперечисленного, а также следует соблюдать элементарные правила безопасности. Ведь, как известно, любую проблему легче предотвратить, чем потом бороться с нежелательными последствиями.