УДК 004.77

Социальная инженерия и защита информации в компьютерных системах и сетях

Ч.М. Шакирянов, МБОУ гимназия им. И.Ш.Муксинова г.Янаул муниципального района Янаульский район Республики Башкортостан.

Технологии безопасности малоэффективны в противостоянии хакерам, использующим методы социальной инженерии. В этой связи актуальной становится проблема работы с персоналом, обучение сотрудников применению политики безопасности и техникам противостояния социальным инженерам, что является залогом безопасности для баз корпоративной информации.

Все реальные примеры социальной инженерии говорят о том, что она легко адаптируется к любым условиям и к любой обстановке, а жертвы социальных хакеров, как правило, даже не подозревают, что по отношению к ним применяют какую-то технику, и тем более не знают, кто это делает.

Все методы социальной инженерии основываются на особенностях принятия людьми решений. Это так называемый когнитивный базис, согласно которому люди в социальной среде всегда склонны кому-то доверять.

Овладеть искусством управления действиями окружающих способен каждый, но эти умения нужно использовать во благо людям. Иногда направлять человека и подталкивать его к выгодным нам решениям полезно и удобно. Но намного важнее уметь определять социальных хакеров и обманщиков, чтобы не стать их жертвой; намного важнее и самому не быть одним из них. Технологии не стоят на месте и с каждым днём системы защиты модернизируются и развиваются. Но человек, всегда остаётся человеком и ему присуще определённые шаблоны поведения, из-за этого в мире совершается огромное количество хакерских атак, целенаправленно использующих эти уязвимости. Социальная инженерия развивалась с древнейших времён, и на каждом этапе развития у неё были свои методы и техники. Подходы к выполнению атак меняются, из-за чего программистам приходится разрабатывать всё новое и новое программное обеспеченье для защиты данных и стабильной работы системы. Единственный способ защитится от социальной инженерии это изучить ее, и научиться применять. Если нужно устранить опасности человеческого фактора, нужно сначала научиться вначале видеть его уязвимости. Ну и по возможности воздействовать на них, дабы знать, чего ожидать. Важно понимание проблемы социальной инженерии и ее высокой опасности для личных и служебных данных. Любой пользователь обязан владеть информацией о том, какие приемы “психологического взлома” могут быть против него использованы и как нужно на них реагировать.