Які основні задачі криптоаналізу потрібно вирішити відносно симетричних криптосистем та при яких вхідних даних вони можуть вирішуватись? Що повинна відображати модель порушника (крипто аналітика) та які його практичні та потенційні можливості?

Основними задачами ***криптоаналізу*** є розробка та ефективне застосування методів, систем, комплексів, алгоритмів і засобів аналізу криптографічних систем. При цьому основною метою криптоаналізу, з точки зору розробника, є визначення криптографічної стійкості криптографічних перетворень, перш за все у сенсі неможливості визначення спеціальних (ключових) даних, протидії несанкціонованому доступу до конфіденційних даних, підробки чи створення хибних повідомлень тощо.

Неформальная модель нарушителя

Нарушитель – это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

Для того, чтобы определить вероятные источники угроз информационной безопасности автоматизированной информационной системы и показатели риска, для этих угроз строится неформальная модель нарушителя. Такая модель отражает потенциальные возможности и знания нарушителя, время и место действия, необходимые усилия и средства для осуществления атаки и т.п. и в идеале должны быть адекватна реальному нарушителю для данной АИС.

Модель нарушителя включает следующие (обоснованные) предположения:

- *О категориях лиц*, к которым *может принадлежать нарушитель*: пользователи системы, обслуживающий персонал, разработчики АИС, сотрудники службы безопасности, руководители – внутренние нарушители; клиенты, посетители, конкуренты, случайные лица – внешние нарушители.
- *О мотивах нарушителя*. Основными мотивами считаются три: безответственность, самоутверждение или корыстный интерес. В первом случае нарушения вызываются некомпетентностью или небрежностью без наличия злого умысла. Во втором случае нарушитель, преодолевая защиту АИС и получая доступ к системным данным, самоутверждается в собственных глазах или в глазах коллег (такой нарушитель рассматривает свои действия как игру «пользователь – против системы»). Наибольшей опасностью обладает третий тип нарушителя, который целенаправленно преодолевает систему защиты, движимый при этом корыстным интересом.
- *Об уровне знаний нарушителя*: на уровне пользователя АИС, на уровне администратора АИС, на уровне программиста, на уровне специалиста в области информационной безопасности.

- *О возможностях нарушителя (используемых методах и средствах)*: применяющий только агентурные методы, применяющий только штатные средства доступа к данным (возможно, в несанкционированном режиме), применяющий пассивные средства (возможность перехвата данных), применяющий активные средства (возможность перехвата и модификации данных).
- *О времени действия*: во время штатного функционирования АИС, во время простоя АИС, в любое время.
- *О месте действия*: без доступа на контролируемую территорию организации, с доступом на контролируемую территорию (но без доступа к техническим средствам), с рабочих мест пользователей, с доступом к базам данных АИС, с доступом к подсистеме защиты АИС.

Неформальная модель нарушителя строится на основе исследования АИС (аппаратных и программных средств) с учетом специфики предметной области и используемой в организации технологии обработки данных. Поскольку определение конкретных значений характеристик возможных нарушителей – в значительной степени субъективный процесс, обычно модель включает несколько обликов возможного нарушителя, по каждому из которых определяются значения всех приведенные выше характеристик. Наличие неформальной модели нарушителя позволяет выявить причины возможных нарушений информационной безопасности и либо устранить эти причины, либо усовершенствовать систему защиты от данного вида нарушений.