АНАЛИЗ СОЦИАЛЬНЫХ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ершов А.С., Губенко Н Е.
Донецкий национальный технический университет

Задачи и цели системы информационной безопасности

Главной целью любой системы информационной безопасности является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, защита законных интересов Заказчика от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений объекта.

Достижение заданных целей возможно в ходе решения следующих основных задач:

1. Отнесение информации к категории ограниченного доступа (служебной тайне);
2. прогнозирование и своевременное выявление угроз безопасности информационным ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
3. создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;
4. создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;
5. создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения информационной безопасности на достижение стратегических целей.

Типы угроз информационной безопасности

1. По природе возникновения.

1.1. Естественные - угрозы, вызванные воздействием на АС и её компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.

1.2. Искусственные - угрозы, информационной безопасности АС, вызванные деятельностью человека.

2. По степени преднамеренности проявления.

2.1. Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала.

2.2. Угрозы преднамеренного действия (например, угрозы действий злоумышленника для хищения информации).

3. По непосредственному источнику угроз.

3.1. Угрозы, непосредственным источником которых является природная среда (стихийные бедствия, магнитные бури, радиоактивное излучение и т. п.).

3.2. Угрозы, непосредственным источником которых является человек.

3.3. Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства.

3.4. Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства.

Пока разработчики непрерывно изобретают всё лучшие и лучшие технологии защиты, делая всё более трудным возможность использовать технические уязвимости, атакующие всё чаще используют человеческий фактор, уязвимость которого активно используют т. н. социальные инженеры, ведь здравомыслящие технологи кропотливо разработали решения по информационной безопасности для минимизации рисков, связанных с использованием компьютеров, а не на их операторов. Несмотря на интеллект, мы люди - вы, я и любой другой - остаёмся самой серьёзной угрозой для любой другой защиты.

Многие коммерческие продукты по безопасности, применяемые в большинстве компаний, главным образом нацелены на защиту от любительского компьютерного вторжения, вроде тех, совершаемых юнцами, известными как скрипт-кидди. Технологии, вроде устройств для аутентификации (для проверки идентичности), контроля доступа (для управления доступом к файлам и системным ресурсам), и системы для обнаружения вторжений (электронный эквивалент сигнализации) естественно необходимы для программы корпоративной безопасности.

Однако одних только технических решений недостаточно для обеспечения максимально возможной защиты корпоративной информации. Очень часто для того, чтобы обойти средства технической безопасности, налётчик, захватчик или социальный инженер должен найти способ обмануть доверенного пользователя, раскрыть информацию или незаметно заставить неподозревающего человека дать ему доступ. Поскольку возможны ситуации, когда доверенный пользователь обманут, подвержен влиянию, то есть его спровоцировали выдать секретную информацию или выполнить действия, создающие уязвимость в безопасности, в которую нападающий мог бы проскользнуть, то во всём мире не найдется таких технологий, которые могли бы защитить бизнес. Так же как криптоанализ может иногда расшифровать текст закодированного сообщения путём обнаружения слабого места в технологии шифрования, социальные инженеры могут использовать обман против ваших работников, чтобы обойти технологии защиты.

Литература

1. http://securitylab.ru/analitics

2. http://web-hack.ru/