МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ашурко Д.В.

Власова Г.А. – кандидат техн.наук., доцент

В настоящее время общество переживает самый настоящий информационный бум, и ценность информации нельзя преувеличить. Еще в самом начале 19-го века Натан Ротшильд утверждал, что «тот, кто владеет информацией, владеет миром». И по сей день эти слова не теряют свою актуальность. Информация окружает человека везде, а сфера услуг давно преобладает над сферой товаров, что в очередной раз подтверждает важность информации. Информация дает компаниям по всему миру столь необходимое конкурентное преимущество. Именно поэтому на сегодняшний день существует потребность в повсеместном использовании в организациях систем информационной безопасности. Одним из способов организации информационной безопасности на предприятии является составление моделей нарушителя информационной безопасности.

Модель нарушителя информационной безопасности представляет собой совокупность предположений об одном или нескольких потенциальных нарушителях информационной безопасности, их квалификации, мотивах и т. д. [1] После построения подобной модели можно адекватно оценить систему информационной безопасности организации и выстроить соответствующую систему защиты.

Модель нарушителя строится на основании информации, полученной от службы безопасности организации и аналитических групп, о существующих способах получения несанкционированного доступа к информации, обстановке в коллективе, ситуации в окружающей среде.

Как правило, модель нарушителя является неформальной и отражает мотивы предполагаемых действий, цели, способы и инструменты, используемые для их достижения [2].

Помимо этого, модели нарушителя могут иметь различные степени детализации. Так, например, можно выделить три типа моделей: содержательная, сценарная и математическая. Содержательная отражает систему принятых организацией мер противодействия, сценарная – типы совершаемых действий по классам и этапам, а математическая используется для количественной оценки принимаемых мер и степени защищенности объекта.

Также стоит отметить, что зачастую строится несколько моделей, соответствующих нескольким типам нарушителей информационной безопасности, производится оценка нарушителей по уровням их квалификации и технической оснащенности.

Существует два типа нарушителей: внутренние и внешние.

К внутренним нарушителям можно отнести пользователей системы, администраторов, программистов, специалистов службы безопасности, а также обслуживающий персонал. Среди причин, по которым внутренний нарушитель может прибегнуть к неправомерным действиям можно отметить ошибки, корыстные интересы, безответственность, месть.

В то же время к числу внешних нарушителей можно отнести клиентов организации, конкурентов, сотрудников ведомственных органов.

К методам, используемым нарушителем можно отнести сбор данных, перехват информации, использование недостатков системы и последующее внедрение в нее.

При этом нарушители могут обладать различным уровнем знания о системе: начиная от базовых и вплоть до непосредственного принятия участия в разработке системы.

Что касается места воздействия на систему, то нарушители могут перехватывать информацию удаленно либо при непосредственно физическом контакте с системой.

В результате анализа полученной информации, составляется модель или «портрет» нарушителя. Так, например, можно предположить, что доступ к системе может желать получить группа хакеров, в распоряжении которых имеется локальная вычислительная сеть, которые будут использовать чужие каналы с высокой пропускной способностью с помощью вредоносных программ с целью внесения искажения в работу системы. Или, например, конкуренты, использующие собственные каналы и вычислительные сети, могут предпринять усилия по блокировке функционирования системы, подрыву имиджа и получения секретной информации о функционировании организации.

Таким образом, модель нарушителя информационной безопасности позволяет оценить степень защищенности информационных систем организации от различных способов воздействия на них. Также, с помощью построенных моделей можно предугадать действия различных потенциальных нарушителей, предупредить их и выстроить соответствующим образом систему защиты информационных систем организации.

Список использованных источников:

Модель нарушителя информационной безопасности. [Электронный ресурс] – Режим доступа: https://studfile.net/preview/5443545/page:4/ – Дата доступа: 10.04.2020.

Модель нарушителя информационной безопасности. [Электронный ресурс] – Режим доступа: http://infoprotect.net/varia/modelyy_narushitelya_informacionnoy_bezopasnosti – Дата доступа: 10.04.2020.

Модель нарушителя. [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_%D0%BD%D0%B0%D1%80%D1%83%D1%88%D0%B8%D1%82%D0%B5%D0%BB%D1%8F – Дата доступа: 10.04.2020.