ЭКОНОМИКА ЗАЩИТЫ ИНФОРМАЦИИ

Горобченко Д.В., Ожог М. С.

Повсеместное внедрение информационных систем во все сферы жизнедеятельности человека обострило проблему охраны прав использования информационных средств производства. Такие инструменты как охрана людьми, физические защитные устройства часто не могут защитить информационные активы предприятий, т.к. информация не может отчуждаться физически, в отличие от материальных средств производства.

Информационные угрозы могут причинить значительный материальный ущерб, который во многих случаях невозможно оценить количественно, например, пошатнувшийся имидж компании, ее репутация и т.д.

Предмет изучения дисциплины защиты информации еще достаточно молод. Наиболее многообещающими направлениями исследований являются вопросы неверной мотивации, экстерналий в обеспечении безопасности, уязвимости информационных систем, а также сетевой топологии и ее роли в обеспечении безопасности.

Все более очевидным становится тот факт, что информация в большинстве случаев подвержена опасности не из-за плохой системы защиты, а из-за недостаточной мотивации людей, отвечающих за сохранность данных. Причиной является так называемый «эффект морального риска»: когда работник, обеспечивающий безопасность информационной системы, не чувствует на себе последствий от воздействия различных угроз, его внимание может быть притуплено, что может иметь катастрофические последствия.

Таким образом, задача обеспечения безопасности выходит за рамки технических наук, разрабатывающих средства и алгоритмы защиты данных. Социология, психология, политология начинают играть роль, не менее важную, чем математика, приборостроение, программирование и т.д.

Экстерналии – экономические явления, лежащие вне сферы экономических интересов предприятия. Информационная промышленность характеризуется множеством различных видов взаимодействия с окружающим миром. Живучесть системы – довольно сложное явление. Она зависит от суммы индивидуальных

усилий людей, которые предпринимают какое-либо участие в процессе обеспечения безопасности. Корректность построения системы безопасности зависит от лица, делающего наименьший вклад в общее дело. Например, самый небрежный программист из команды разработчиков может сильно повлиять на возможности и уязвимость ПО при его разработке. А тестирование этого же программного продукта зависит от суммы усилий всей команды.

Уязвимость является важным аспектом идентификации угроз, т.к. может привести к ущербу в момент опасности. Риск нарушения безопасности систем не может быть установлен без знания того, насколько уязвима система по отношению к потенциальным угрозам. Неверно определенное значение риска ведет к неправильной оценке возможных последствий в случае угрозы.

Топология сети – это логическая схема соединения каналами связи компьютеров (узлов сети). Она является немаловажным фактором при анализе информационной безопасности систем. Свободно расширяемые сети трудно уязвимы для случайных атак, но могут быть повреждены при направленной атаке на жизненно важные узлы. Результаты последних исследований показали, что наиболее уязвимой является кольцевая топология.

Несмотря на бурное развитие новых высоких технологий, за последние десятилетия средства защиты информационных ресурсов не получили широкое распространение. Множество информационных систем различных фирм и организаций постоянно испытывают на себе последствия от вредоносных воздействий извне. Хотя за последние десятилетия были разработано большое количество инструментов и методологий по защите информации, однако эффективность их использования за все это время осталась практически на том же уровне. Специалисты предполагают, что основными причинами здесь выступает неверная мотивация и неправильная организация. Также необходимо понимать, что одно лишь наличие средств защиты информации еще не дает гарантии ее сохранности. Помимо всего прочего, необходимо научится эффективно и рационально использовать эти средства.