ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Сурнин А.П.
Кафедра систем управления
Научный руководитель: Сорока Н.И., доцент кафедры СУ, канд. техн. наук, доцент
e-mail: notdennis@rambler.ru

***Аннотация* — Доклад посвящен анализу проблемы оценки эффективности систем защиты информации. Рассмотрены основные подходы к оценке эффективности, их преимущества и недостатки. Предложена методика выбора количественных показателей эффективности.**

Ключевые слова: защита информации, показатель эффективности, системный подход

В настоящее время для обеспечения защиты информации в информационных системах внедряются строго регламентированные организационные мероприятия, а также применяются дорогостоящие аппаратные и программные средства. Однако, несмотря на то, что защита критически важных для собственников информационных систем соответствует разнообразным международным и национальным нормативным и методическим документам, достаточно сложно ответить на важный вопрос – насколько эффективна реальная система защиты по сравнению с альтернативными вариантами?

Под эффективностью в общем случае следует понимать степень соответствия результатов защиты информации поставленной цели. Степень достижения цели оценивается при помощи показателей эффективности, выбираемых исходя из задач исследования систем. Выбранный показатель эффективности должен при этом отвечать основным требованиям к показателям эффективности любых технических систем:

1. Показатель должен иметь технический смысл.
2. Показатель должен в полной мере отражать целевое назначение системы.
3. Показатель должен быть количественным (измеряться числом или группой чисел).
4. Количественный показатель должен быть эффективен в статистическом смысле – иметь допустимый разброс измеряемых значений относительно заданной величины.

Примером показателя эффективности является криптостойкость шифра. Для шифра DES этот показатель зависит от одного параметра – разрядности ключа.

Эффективность защиты информации оценивается как на этапе ее разработки, так и в процессе эксплуатации. Можно выделить три основных подхода к оценке эффективности, которые отличаются используемыми показателями и способами их получения [1]:

1. Классический – при таком подходе интегральный показатель формируется на основании нескольких частных показателей, причем их выбор осуществляется исходя из субъективной оценки их значимости.
2. Официальный – в этом случае в нормативных документах приводятся требования к защищенности информации различной степени конфиденциальности и важности. Основной недостаток этого метода в том, что определяется лишь факт наличия или отсутствия конкретного механизма защиты, но не определяется его эффективность.
3. Экспериментальный – при данном подходе моделируются действия по преодолению механизмов защиты системы. Такой подход требует серьезных материальных и временных затрат.

Наряду с тремя рассмотренными подходами можно выделить системный подход, который целесообразно использовать не только для оценки эффективности, но и для непосредственно проектирования и разработки системы защиты информации. Сущность системного подхода заключается в построении достаточно простой, обозримой модели исследуемой системы, которая позволяет определить влияние различных факторов на показатели эффективности системы.

При системном подходе для определения показателя эффективности системы защиты информации следует установить его однозначное соответствие с целью защиты и ресурсами, предназначенными для ее достижения. Данное соответствие можно установить при помощи метода, предусматривающего декомпозицию понятий цели, ресурсов и показателя эффективности системы [2]. Декомпозицию каждого из понятий целесообразно осуществлять построением соответствующих иерархических графов. Таким образом, исследование по оценке эффективности защиты информации можно разбить на два этапа:

1. Анализ цели защиты информации (метод декомпозиции).
2. Синтез интегрального показателя эффективности на основе итерационной процедуры с уточнением результатов анализа.

Полученный показатель эффективности, который имеет вероятностный смысл, позволит объективно характеризовать степень защиты информации в условиях случайных или преднамеренных воздействий.

[1] Завгородний, В.И. Комплексная защита информации в информационных системах / В.И. Завгородний. – М.: Логос, 2001. – 264 с.: ил.

[2] Бузов, Г.А. Защита от утечки информации по техническим каналам / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М.: Горячая линия-Телеком, 2005. – 416 с.: ил.