Н.М. Бобович

ОБ ОЦЕНКЕ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

В концепции национальной безопасности Республики Беларусь наряду с другими в качестве приоритетных определены следующие направления обеспечения безопасности Республики Беларусь в информационной сфере:

разработка и внедрение современных методов и средств защиты информационных технологий, прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;

осуществление государственного контроля за разработкой, созданием, развитием и использованием средств защиты информации;

обеспечение правовых и организационных условий предупреждения, выявления, пресечения преступлений в информационной сфере.

Успешная реализация указанных направлений зависит от разрешения проблемы достоверной оценки эффективности систем и средств защиты информационных технологий (систем защиты информации), характеризующей степень соответствия результатов защиты информации поставленной цели.

Количественная оценка эффективности систем защиты информации (СЗИ) необходима для решения следующих задач:

принятие решения о допустимости практического использования СЗИ в конкретной ситуации;

выявление вкладов различных факторов в достижение цели;

установление путей повышения эффективности СЗИ;

сравнение альтернативных вариантов систем.

Как показывает анализ существующей методологии, оценка эффективности СЗИ носит, как правило, нечеткий, субъективный характер, а необходимые для этой оценки нормированные количественные показатели практически полностью отсутствуют. Следствием этого является то, что в ряде случаев сложно, а часто и невозможно, оценить качество функционирования СЗИ в условиях воздействия дестабилизирующих факторов (ДФ) и определить, чем один вариант применяемой системы лучше другого.

В зависимости от показателей и способов их получения, используются следующие подходы к оценке эффективности СЗИ:

официальный;

экспериментальный;

классический.

Официальный подход характеризуется тем, что требования к защищенности различных категорий конфиденциальности и важности определяются нормативными правовыми актами Республики Беларусь, где задаются перечни механизмов защиты информации, которыми должна располагать защищаемая ИС, чтобы она соответствовала определенному классу защиты. По существу критерием эффективности СЗИ в этом случае является ее класс защищенности. Очевидным недостатком официального подхода к определению эффективности СЗИ является отсутствие возможности определения эффективности конкретного механизма защиты, так как констатируется только факт его наличия или отсутствия.

Экспериментальный подход к оценке защищенности информационной системы предполагает планирование и выполнение последовательности экспериментов по взламыванию защитных механизмов специалистами, выступающими в роли злоумышленников. При этом имеется возможность получить достаточно объективные данные о возможностях испытываемых средств защиты, но требуется участие высококвалифицированных специалистов при больших материальных затратах.

При классическом подходе оценка эффективности защиты осуществляется по критериям эффективности с использованием показателей эффективности путем моделирования (вычисления) по характеристикам реальной информационной системы. Несомненным преимуществом классического подхода является возможность количественной оценки (измерения) эффективности СЗИ и последующего сравнения. Это, в свою очередь, позволяет синтезировать эффективные СЗИ и анализировать влияние отдельных механизмов защиты на область управления защитой ИС.

В качестве показателей для количественной оценки эффективности защиты используются:

защищенность (вероятность того, что объект защиты будет защищен от определенных угроз или дестабилизирующих факторов);

предотвращенный ущерб (величина предотвращенного с помощью СЗИ ущерба);

относительный предотвращенный ущерб (величина предотвращенного ущерба, соотнесенная с величиной затрат на применение СЗИ).

Среди перечисленных показателей наибольшее распространение получил предотвращенный с помощью СЗИ ущерб, потенциальная величина которого зависит как от уровня защищенности, так и от интенсивности атак и ценности информации в защищаемой системе.

Количественная оценка эффективности СЗИ по показателю «предотвращенный ущерб» осуществляется с помощью следующего выражения:

$$W = \frac{L - R}{R},$$

где L – усредненная величина предотвращенного ущерба;

R – приведенные затраты на создание и функционирование СЗИ (на защиту) при предотвращении такого ущерба ($R \neq 0$).

Поскольку на практике допустимые затраты на защиту ограничены $\left(R \le R_{\text{доп}}\right)$, то можно сформулировать обобщенный критерий эффективности СЗИ: значение потенциального предотвращенного ущерба L, который может быть нанесен ИС, не должен превышать допустимого уровня $L_{\text{тр}}$ $\left(L \ge L_{\text{тр}}\right)$ при ограниченных затратах R на реализацию СЗИ СОИ $R \le R_{\text{доп}}$.

Если в качестве частных показателей эффективности зашиты воспользоваться значениями предотвращенного потенциального ущерба L_Z – для каждого возможного состояния S_Z, $Z = \overline{1, Z}$ и затрат на реализацию СЗИ – R, то в качестве обобщенного критерия эффективности защиты может быть принято условие, что СЗИ удовлетворяет частным критериям:

$$\left\lfloor L_Z \ge L_{Zmm} R \le R_{\text{доп}} \right\rfloor,\ Z = \overline{1, Z},$$

где L_{Zmm} – требуемое значение предотвращенного ущерба;

$R_{\text{доп}}$ – допустимые затраты на реализацию защиты.

Выбранные показатели эффективности и критерий оптимального выбора механизмов безопасности элементов ИС позволяют представить процедуру определения наилучшего варианта СЗИ в виде следующего алгоритма:

1. Из области управления защищенностью ИС формируется полный перечень доступных механизмов безопасности

$$D = \{ D_1, D_2, \ldots, D_i, \ldots, D_k \}.$$

2. Определяются все возможные варианты построения СЗИ: S_i, $i = \overline{1, 2^{k-1}}$.

3. Для каждого варианта СЗИ определяются частные показатели эффективности защиты L_i, R_i.

4. Определяется наилучший вариант построения СЗИ по критерию

$$W = \frac{L_i - R_i}{R_i} \to \max,\ i = \overline{1,\ 2^{k-1}}.$$

Таким образом, на основании выбранного показателя эффективности предложен алгоритм выбора механизмов безопасности для построения наилучшей системы защиты информации ИС. Реализации этого алгоритма должен сопутствовать подробный анализ относительно полного множества практически достижимых дестабилизирующих факторов, исследовано множество механизмов защиты элементов СОИ на предмет их прочности.

П.В. Бондарь

О НЕОБХОДИМОСТИ РАЗРАБОТКИ МЕТРИК ПОКАЗАТЕЛЕЙ КАЧЕСТВА ПРОГРАММНЫХ СРЕДСТВ, РЕАЛИЗУЮЩИХ СТАНДАРТИЗОВАННЫЕ КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ

Программные средства (ПС), реализующие стандартизованные средства криптографической защиты информации (КЗИ), являются одним из ключевых элементов обеспечения безопасности информационных технологий. Оценка качества таких ПС должна базироваться на расчетных соотношениях и быть максимально независимой от субъективных оценок экспертов. Объективные числовые характеристики, основанные на метриках качества, позволяют не только оценивать функциональность ПС, но и сравнивать различные программные реализации одного и того же алгоритма КЗИ.

При определении показателей качества ПС необходимо учитывать как требования ГОСТ 28195, так и требования базовых международных стандартов, систематизирующих и регламентирующих качество ПС, в частности, ISO/IEC 9126:1-4 (ISO/IEC 25021–25024). Указанные международные стандарты (в Республике Беларусь действует СТБ ИСО/МЭК 9126) устанавливают ряд метрик для объективной оценки ПС, однако метрики для оценки качества реализаций средств КЗИ представлены в них в недостаточном объеме. Кроме того, установленный в ISO/IEC 9126 подход к вычислению значений метрик показателей качества является упрощенным и не позволяет объективно и в полной мере оценить качество ПС.

Вычисление значений метрик показателей качества, применяемое в ISO/IEC 9126, сводится к вычислению отношения числа испытаний, в которых зафиксировано наступление некоторого события, к общему числу проведенных испытаний. Полученное отношение может принимать значение от 0 до 1. По сложившейся практике результаты проверки ПС, реализующего алгоритм КЗИ, считаются положительными, ес-