Сама по собі схема рис. 3 не може дати повного уявлення про наведений алгоритм (звичайно на відміну від його текстового опису). Однак, якщо схему доповнити текстовим описом (за основу все ж взяти ПСО-схему, а не навпаки), то розбір алгоритму значно спрощується. Основні його стадії можна легко зрозуміти зі схеми, а при виникненні уточнюючих питань, звернутися до текстового опису, з яким у ПСО-схеми встановлено взаємно однозначну відповідність.

Аналізуючи рис. 3 можна встановити ще одну принципову особливість ПСО-схем. Для цього звернемо увагу на дію 3, яка в цілому представляє окремий сам по собі складний процес, що може оперувати своїми об'єктами за допомогою своїх суб'єктів. Отже, ПСО-схеми можуть легко каскадуватися за рівнями деталізації, тобто можемо розглядати схему алгоритму високого рівня, у якого деякі стрілки (дії) потім можуть деталізуватися у вигляді своїх окремих ПСО-схем. Таким чином, зручно реалізується принцип проектування зверху-вниз.

Висновки

Розроблено методику графічного представлення алгоритмів роботи СЗІ у вигляді процесно-суб'єктно-об'єктних схем. ПСО-схеми дають чітке уявлення про послідовність дій алгоритму, реалізують наочне представлення суб'єктів та об'єктів, що є складовими частинами СЗІ, а також потоків інформації між ними. За допомогою ПСО-схем можна легко встановлювати логіку роботи програмних СЗІ, аналізувати або синтезувати необхідні алгоритми, переходячи між різними рівнями деталізації. В якості реального прикладу використання створеної методики, зображено алгоритм роботи авторської СЗІ, що здійснює контроль цілісності підсистеми фізичного захисту ПЗ.

Список літератури

1. ГОСТ 19.701-90. Схемы алгоритмов и программ. Обозначения условные графические.

2. *Евстигнеев В.А.* Применение теории графов в программировании. / Под ред. А.П. Ершова. – М.: Наука, 2000. – 352 с.

3. *Калянов Г.Н.* Структурный системный анализ (автоматизация и применение). – М.: Издательство "ЛОРИ", 1996.

4. *Гальчевський Ю.Л., Гайша О.О.* «Логічні» та «фізичні» захисти програмного забезпечення від несанкціонованого копіювання // Захист інформації: Науково-технічний журнал. – 2005. – №2(23). – С. 34-40.

Надійшла 20.12.2006 р.

УДК 65.012.8: 004.492

Гроздов Г.Г.

МЕТОДИКА ОПРЕДЕЛЕНИЯ ПОКАЗАТЕЛЯ ЭФФЕКТИВНОСТИ МЕХАНИЗМОВ ЗАЩИТЫ ИНФОРМАЦИИ

В настоящее время актуальна задача построения и оценки эффективности механизмов защиты информации в различных комплексных системах защиты информации (КСЗИ) автоматизированных систем (АС).

Можно выделить такие классы информации, защита которых должна обеспечиваться механизмами защиты информации (ЗИ), входящими в состав КСЗИ: информация, составляющая коммерческую и военную тайну. В АС указанных классов могут иметь приоритетное значение различные требования к механизмам ЗИ [1, 2].

В научно-технической литературе рассматриваются два аспекта эффективности системы ЗИ. С одной стороны, система защиты информации должна эффективно

противодействовать угрозам [3, 4]. С другой стороны, она должна быть адекватной – расходы на безопасность не должны превышать стоимости самой информации и размера возможных потерь, вызванных успешной реализацией угроз [3, 5].

Существующие подходы оценки эффективности защиты информации, их недостатки

К наиболее известным методикам оценки экономической эффективности КСЗИ относятся метод ожидаемых потерь [6, 7] и методика совокупной стоимости владения [7, 8]. Популярность этих методик можно объяснить тем обстоятельством, что они применяются в случаях оценки КСЗИ АС, обрабатывающих информацию, составляющую коммерческую тайну. Указанные методики имеют ряд недостатков:

- метод ожидаемых потерь рассматривает риски как математическое ожидание потерь. Эта методика не учитывает многих факторов, оказывающих влияние на безопасность информации [9]. Например, не были учтены потери, которые могла понести АС вследствие применения механизмов защиты информации [2];
- метод ожидаемых потерь и методика совокупной стоимости владения эффективны для оценки СЗИ АС, обрабатывающих информацию, составляющую коммерческую тайну и не учитывают многих аспектов защиты информации, составляющую государственную тайну.

В работе [10] предлагается многокритериальный метод оценки эффективности механизмов защиты информации. Суть метода состоит в экспертной оценке различных показателей механизма защиты информации. Кроме того, эксперты могут определить значимость отдельных показателей. Методика позволяет оценить эффективность практически любого механизма ЗИ. Однако у предложенной методики имеется ряд недостатков:

- по мнению автора, недостаточно четко описаны параметры механизма ЗИ, подлежащие оцениванию;
- предложенная методика не учитывает требования нормативных документов по вопросам ЗИ.

Постановка целей исследования

Исходя из вышеизложенного, задачи исследования могут быть сформулированы таким образом:

- разработку методики оценки эффективности механизмов ЗИ.
- разработка методик вычисления эффективности совместного применения двух или более механизмов ЗИ.

Методика оценки эффективности механизмов защиты информации

В соответствии с [11], к любому механизму ЗИ выдвигаются требования двух видов: к услугам безопасности и уровню гарантий реализации.

Любой механизм ЗИ рассматривается как набор функциональных услуг. Каждая услуга представляет собой набор функций, которые позволяют противостоять определенному множеству угроз. В соответствии с нормативными документами ТЗИ, каждая услуга может включать несколько уровней. Чем выше уровень услуги, тем более полно обеспечивается защита от определенного вида угроз. Функциональные критерии разбиты на 4 группы. Каждая из групп описывает требования к услугам, которые обеспечивают защиту от угроз одного из четырех основных типов: конфиденциальности, доступности, наблюдаемости и целостности.

Алгоритм оценки величины G показан на рис. 1.

В процессе оценки возможностей механизма защиты информации, группа экспертов формирует вектор D (параметры указанных переменных описаны в таблице 1).

Эксперт во время оценивания учитывает функциональный профиль защищенности (далее - ФПЗ) механизма защиты, а также его гарантии реализации (далее - ГР).

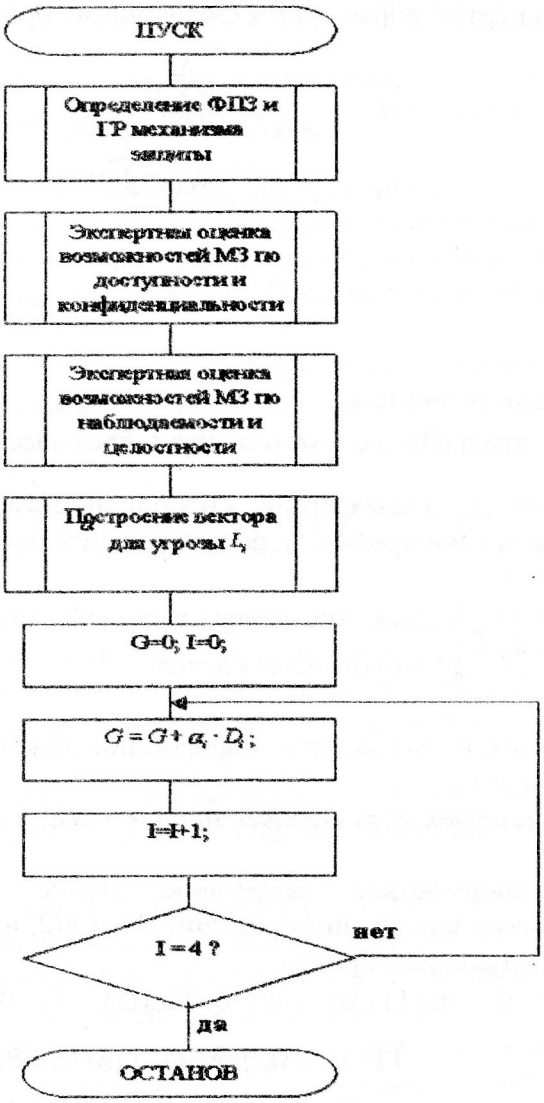

Рис. 1. Алгоритм формирования величины G для механизмов защиты информации

Таблица 1

Параметры переменных, используемых в методике формирования показателя эффективности j-го механизма защиты информации

Обозначения переменных	Значения переменных	Ограничения переменных
D[i]	средняя оценка экспертов возможностей механизма защиты свойств информации i=0; доступности i=1; конфиденциальности i=2; наблюдаемости i=3; целостности	$0 < D[i] < B_{max}$
α[i]	возможности угрозы по нарушению свойств информации АС i=0; нарушение доступности i=1; нарушение конфиденциальности i=2; нарушение наблюдаемости i=3; нарушение целостности	$\alpha[i] \in (0;1)$

Средняя оценка экспертов формируется следующим образом:

$$Y = \frac{\sum_{i=1}^{N} B_i}{N \cdot B_{\max} \cdot \sum_{i=1}^{4} \alpha_i},$$

где Y - средняя оценка;

N - число экспертов;

α_i - свойства угрозы;

B_I - оценка, поставленная экспертом;

$B_{\max}$ - максимальная оценка в баллах, которая может быть выставлена при оценивании.

Для описания свойств угрозы формируется бинарный вектор α. Возможности угрозы описываются таким образом (на примере угрозы доступности).

$$\alpha_0 \uparrow \begin{cases} 1, \text{если угроза нарушает свойства доступности;} \\ 0, \text{в противном случае;} \end{cases}$$

Величина G для механизма защиты информации может быть получена как скалярное произведение векторов α и D.

Оценка эффективности совместного использования двух и более механизмов защиты информации

Если для противодействия какой-либо угрозе информации предполагается использовать два механизма защиты информации: *M1* и *M2*, их обобщенные характеристики могут быть получены следующим образом.

$$\text{ФПЗ}(M1+M2)=\text{ФПЗ}(M1) \quad \text{Y} \quad \text{ФПЗ}(M2);$$

$$\text{ГР}(M1+M2)=\text{Min}(\text{ГР}(M1), \text{ГР}(M2));$$

$$C(M1+M2)=C(M1) + C(M2);$$

где C - цена механизма ЗИ.

Подробнее остановимся на возможных диапазонах величины G. В случае отсутствия каких-либо услуг безопасности в составе ее ФПЗ применение указанной методики даст нулевое значение. Максимальным значением указанной величины может быть 1. Однако достижение такого значения в современных условиях автору представляется маловероятным по следующим соображениям:

- большинство из существующих механизмов защиты информации обладают невысоким уровнем гарантии реализации;
- многие из механизмов защиты информации, существующих в Украине, не обладают высоким уровнем реализации услуг безопасности.

Указанное обстоятельство значительно снижает уровень оценки величины G по предлагаемой методике.

Выводы из исследования и перспективы дальнейших разработок

Разработана методика оценки эффективности механизмов ЗИ в АС. В отличие от существующих, методика учитывает функциональный профиль защищенности и уровень гарантий реализации механизма ЗИ.

Отметим направления перспективных разработок для оценки эффективности механизмов ЗИ:

- новые методики должны учитывать снижение эффективности механизмов ЗИ с течением времени их использования;
- эффективность механизмов защиты информации должна также зависеть от возможностей вероятного противника, пытающегося нанести ущерб АС (объекту защиты).

Список литературы

1. *Гроздов Г.Г.* Новая постановка задачи формирования экономически эффективной комплексной системы защиты информации в автоматизированных системах первого и второго класса // Научно- технический журнал "Электроника и системы управления", 2005, № 4. Киев - 2005, - С. 88-96.

2. *Гроздов Г.Г.* Способ решения задачи формирования комплексной системы защиты информации для автоматизированных систем 1 и 2 класса: Препр./ НАН Украины. Отделение гибридных моделирующих и управляющих систем в энергетике ИПМЭ им Г.Е.Пухова; - К.: 2005. -№1. - 66 с.

3. *Герасименко В.А, Размахнин М.К, Диев С.А.* Новые данные о защите информации в автоматизированных системах обработки данных. // Зарубежная радиоэлектроника .-1987. - № 9. - С. 48-75.

4. *Гроздов Г.Г.* Постановка задачи формирования комплексной системы защиты информации в автоматизированных системах первого и второго класса. // Научно-технический журнал "Электронное моделирование". -2006. - №2, - С. 43-54.

5. *Скрипкин К.Г.* Экономическая эффективность информационных систем. - М. : ДМК, 2002. - 252 с.

6. *Арзуманов С.В.* Оценка эффективности инвестиций в информационную безопасность. // Научно-технический журнал "Защита информации. INSIDE". -2005.- №1. - С. 23-25.

7. *Петренко С.А., Терехова Е.М.* Обоснование инвестиций в безопасность. // Научно-технический журнал "Защита информации. INSIDE".-2005.- №1. - С. 49-53.

8. *Петренко С.А., Терехова Е.М.* Оценка затрат на защиту информации. // Научно-технический журнал "Защита информации. INSIDE".-2005.- №1. - С. 36-47.

9. *Медведовский И.* Современные методы и средства анализа и контроля рисков информационных систем компаний. - Электрон. дан.- Режим доступа: Http://Www.Citforum.Ru/Products/Dsec/itrisk. - Загл. с экрана.

10. *Фаткиева Р.Р.* Метод многокритериальной оценки эффективности средств защиты информации. - Электрон. дан. - Режим доступа: http://www.spiiras.nw.ru /Fatkieva140105.ppt - Загл. с экрана.

11. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - К.: ДСТСЗИ СБ Украины, 1999. - 58 с.

НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. - К.: ДСТСЗИ СБ

Поступила 12.10.2006 г.
После доработки 28.11.2006 г.