УДК 004.621:519.872.3

С.Ж. Пискун,
В.А. Хорошко

ОПТИМИЗАЦИЯ ВЫБОРА ФУНКЦИОНАЛЬНОГО ПРОФИЛЯ ЗАЩИЩЕННОСТИ

Формализована задача выбора оптимального профиля защищенности. Детально описаны основные характеристики задачи.

Ключевые слова: *система защиты информации, стандартный функциональный профиль защищенности, объект защиты.*

Формалізовано завдання вибору оптимального профілю захисту. Детально окреслено основні характеристики завдання.

Ключові слова: *система захисту інформації, стандартний функціональний профіль захисту, об'єкт захисту.*

The problem of a choice of an optimum profile of security is formalized. The basic characteristics of a problem are described in details.

Keywords: *information security system, standard functional profile, object of protection.*

Создание любой системы защиты информации (СЗИ) во всех сферах информационной деятельности общества включает обязательную процедуру выбора и последующую реализацию (СФПЗ) [1–4]. В задачу разработки входит обследование свойств конкретного объекта защиты (ОЗ) и выбор необходимого СФПЗ из приведенного [3] сигнала. Там же дается рекомендация, что если ни один СФПЗ из приведенного сигнала не подходит к конкретному ОЗ, разработчик может создать свой, наиболее подходящий для него, СФПЗ, обследовать и утвердить его.

В работе [5] предложен подход к решению этой задачи, который базируется на формализованном отношении свойств ОЗ и свойств СФПЗ и дальнейшем использовании взаимно однозначной зависимости между этими свойствами. Для установления этой зависимости используется уже известный список СФПЗ, что и позволяет определить наиболее подходящий СФПЗ для данного ОЗ. Однако не всегда удается четко формализовать свойства ОЗ и установить связь между ними и необходимым СФПЗ.

В работе [6] предложена формальная постановка задачи синтеза оптимальной СЗИ, позволяющая определить наиболее рациональный вариант технической реализации СЗИ. Этот подход может быть использован для формулирования задачи выбора оптимального СФПЗ.

Согласно нормативным документам [1–4] каждый СФПЗ является набором соответствующих функциональных услуг. Каждая услуга является набором функций, позволяющих противостоять определенному множеству угроз, причем каждая услуга может включать несколько уровней. Чем выше уровень услуги, тем более сложно

обеспечивается защита от определенного вида угроз. Уровни услуг имеют иерархию по полноте защиты, хотя и не являются точными под-множествами друг друга. Уровни начинаются с первого и возрастают до уровня п, где п – определенное для каждого вида услуг число.

На современном уровне развития информационных технологий и с учетом намеренных требований и потребностей информационной безопасности на ОЗ определено 22 вида услуг. Они обеспечивают защиту от четырех основных типов угроз (конфиденциальности, целостности, доступности и наблюдаемости).

При создании ОЗ различного назначения у разработчика возникает вопрос: какие именно услуги и каких уровней следует принимать во внимание. СФПЗ – это минимальный набор определенных услуг определенных уровней для обеспечения определенного уровня защищенности. Выбор способов их реализации остается за разработчиком. При создании каждого СФПЗ из известного списка их разработчики учитывали, что услуги определенных уровней должны входить в их состав в соответствии с заданными для определяемого ОЗ логикой, требованиями, принципами и ограничениями. Очевидно, что, в первую очередь, учитывались такие сведения об ОЗ, как его списка и основные требования к защищаемой информации (преимущественное обеспечение конфиденциальности; целостности; доступности; конфиденциальности и целостности; конфиденциальности и доступности; целостности и доступности; конфиденциальности, целостности и доступности). Кроме того, необходимо принимать во внимание типы ОЗ, уровень секретности обрабатываемой информации и другие показатели, которые характеризуют ОЗ и информацию циркулирующую на нем. При этом должен быть обеспечен заданный уровень защищенности, а затраты на СЗИ должны быть минимизированы.

Таким образом, видно, что СФПЗ является, по существу, вариантом технической реализации СЗИ ОЗ [5–7].

При формализации задачи выбора оптимального СФПЗ необходимо использовать такие показатели, как вероятность появления угроз, вероятность устранения угроз, предотвращения ущерба за счет ликвидации угроз.

Для этого рассмотрим математическую модель СФПЗ. Пусть – множество всех возможных СФПЗ. Под будем понимать вектор размерности 22 – именно столько услуг сейчас определено. Такая размерность введена для удобства и унификации описания СФПЗ, поскольку известно, что в состав многих СФПЗ входят не все услуги. В случае отсутствия какой-либо услуги соответствующая компонента просто приравнивается нулю.

За счет реализации необходимого СФПЗ обеспечивается уменьшение ущерба, наносимого ОЗ. Обозначим общий предотвращенный ущерб ОЗ через S(P).

Формальная постановка задачи имеет вид:

$$P_0 = \underset{P_0 \in \overline{P}}{argmax} S(P) \qquad (1)$$

при ограничении

$$C(P_0) < Cr. \qquad (2)$$

Здесь P – некоторый вектор, характеризующий СФПЗ, $\bar{P}$ – множество допустимых профилей, P_0 – оптимальное значение вектора P, Cr – допустимые затраты на СФПЗ.

В соответствии с материалами, приведенными в [8–9], каждая угроза информации является следствием реализации некоторого множества факторов называемых дестабилизирующими. Предположим, что злоумышленник имеет возможность реализовать некоторое множество дестабилизирующих факторов, в результате чего может возникнуть множество угроз t_i, i=1,.....,n (заметим, что n=4). Каждую i-ую угрозу будем характеризовать вероятность ее появления P_{it} и ущербом, наносимым информационной среде S_i .

Угрозы должны нейтрализоваться соответствующими средствами и механизмами СЗИ, которые обеспечиваются реализацией функциональных услуг. При этом основной характеристикой СЗИ будет вероятность нейтрализации каждой i-ой угрозы. Поскольку функциональные угрозы составляет СФПЗ, то вероятность нейтрализации каждой i-ой угрозы P_{is}. Поскольку функциональные услуги составляют СФПЗ, то, очевидно, что вероятность нейтрализации i-ой угрозы должна зависеть от вектора СФПЗ, т.е. является функцией $P_{is}=g_i(P)=g_i(P_1,...,P_m)$, где, как было ранее отмечено, m=22. Разложив в ряд до линейного члена данные функции получим:

$$P_{is} \approx g_i(0,\ldots\ldots,0 + \sum_{i=1}^{m} \frac{\delta g_i}{\delta P_i} P_i \qquad (3)$$

Далее, считая по определению $g_i(0,...,0)$, окончательно получим

$$P_{is} \approx \sum_{j}^{m} = 1 \frac{dg_i}{dP_j} P_j, \qquad (4)$$

где каждая j-ая производная может интерпретироваться как степень влияния требования на вероятность реализации j-ой услуги (вероятность выполнения j-ой требования для реализации j-ой услуги). На них необходимо наложить следующие ограничения

$$0 \le \frac{\partial g_i}{\partial P_j} \le 1, \quad \sum_{j}^{m} = 1 \frac{\partial g_i}{\partial P_j} = 1, \quad i=1,\ldots\ldots,n \qquad (5)$$

Их величины определяются экспертным путем. Экспертным путем определяются и все остальные компоненты вектора СФПЗ

$$P_i, \; i=1,\ldots\ldots, \; m.$$

За счет реализации необходимо СФПЗ обеспечивается уменьшение ущерба наносимого ОЗ воздействиям угроз. Обозначим общий предотвращенный ущерб ОЗ через S, а предотвращенный ущерб за счет предотвращения i-ой угрозы через r_i.

Предотвращенный ущерб выражается в общем виде соотношением:

$$S(P) = \sum_{j=1}^{n} P_j P_{ji} S_j. \qquad (6)$$

Предотвращенный ущерб за счет ликвидации воздействия i-ой угрозы:

$$r_i = P_i P_{it} S_i. \quad (7)$$

Вероятность появления i-ой угрозы P_{it} определяется следующим образом. Как было указано ранее, каждая угроза зависит от вероятностей реализации некоторого множества дестабилизирующих факторов $Di = \{dij, i = 1,...,n\}$, т.е. $P_{it} = f_i(d_{ij},...,d_{inj})$. Считая, что для каждого i=1,...,п указанные функции являются достаточно гладкими, получим их разложения в ряд (до линейных членов):

$$P_{it} \approx f_i(0,...,0) + \sum_{j=1}^{m_i} \frac{\partial f_i}{\partial d_{ij}} d_{ij}, \quad (8)$$

Поскольку $f_i(0,...,0) = 0$, то окончательно

$$P_{it} \approx \sum_{j=1}^{m_i} \frac{\partial f_i}{\partial d_{ij}} d_{ij}, \quad (9)$$

где каждая j=ая производная интерпретируется как степень влияния требования на вероятность нейтрализации j-го дестабилизирующего фактора (важность выполнения j-го требования для нейтрализации j-го дестабилизирующего фактора). При этом

$$0 \le \frac{\partial f_i}{\partial d_{ij}} \le 1, \quad \sum_{j=1}^{m_i} \frac{\partial f_i}{\partial_{ij}} = 1, \quad i = 1,..., n. \quad (10)$$

Вероятность появления d_{ij} j-го дестабилизирующего фактора могут определяться статистически и практически соответствуют относительным частотам их появления

$$d_{ij} = \frac{\lambda_{ij}}{\sum_{k=1}^{n_i} \lambda_{ik}}, \quad (11)$$

где λ_{ij} – частота появления j-го дестабилизирующего фактора, а i везде относится к соответствующему номеру угрозы. Величины производных определяются экспертным путем. Ущерб S_i, наносимый i-ой угрозой, может определяться в абсолютных единицах: экономических потерях, временных затратах, снижении уровня защищенности, объема уничтоженной или поврежденной информации и т.д.

Исследована постановка формальной задачи оптимального выбора стандартного функционального профиля защищенности для ОЗ, а также показаны возможности детального отношения основных показателей, необходимых для этого: вероятность появления угроз, вероятность устранения угроз, предотвращенный ущерб за счет нейтрализации угроз. Основными этапами решения этой задачи следует считать:

– сбор и обработку экспертной информации об угрозах: ущерб, частоту появления;

– оценку стоимости системы защиты для конкретного стандартного функционального профиля защищенности с учетом ограничения $C(P_0) < Cr$.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. НД ТЗІ 1.1 – 005 – 07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

2. НД ТЗІ 2.5 – 005 – 99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

3. НД ТЗІ 3.3 – 001 – 07. Захист інформації на об'єктах інформаційної діяльності. Створення технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

4. ДСТУ ISO/IES TR 13335 – 1: 2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій.

5. *Браиловкий Н.Н.* Оценка качества функционирования систем защиты информации / Н.Н. Браиловский, В.С. Орленко, В.А. Хорошко // Сучасний захист інформації. – 2010. – № 4. – С. 9–15.

6. *Капустян М.В.* Кількісна оптимізація інформаційних структур нормативних мереж / М.В. Капустян, В.А. Кудіков, Л.Т. Пархуць, В.А. Хорошко // Комп'ютерні технології друкарства. Збірник наукових праць. – 2006. – № 16. – С. 24–34.

7. *Хорошко В.А.* Каналы информационного воздействия / В.А. Хорошко, В.С. Чередниченко // Зб. наук. праць ВІКНУ ім. Т. Шевченка. – 2008. – Вип. 11. – С. 65–71.

8. *Ленков С.В.* Методы и средства защиты информации. В двух томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К. : Арий, 2008.

Отримано 02.09.2011