можно записать как

$$\boldsymbol{M} \sim mod\ \boldsymbol{T}.$$

Тогда при решении практических задач приведенное выше соотношение дает право учитывать в процессе составления нормативных документов по управлению обеспечения защитой информации в АС описание свойств класса ***M.***

Литература: ***1****. Расстригин Л. А. Адаптация сложных систем. Методы и приложения. – Рига: Зинатне, 1981. – 375 с.* ***2****. Общие критерии оценки безопасности информационных технологий: Уч. пособие. Пер. с англ. Е. А. Сидак / Под ред М. Т. Кобзаря. – М.: МГУЛ, 2001. – 81 с.* ***3****. Зубов В. И. Лекции по теории управления. М.: МГУ, 1975. –496 с.* ***4****. Романов О. І., Лівенцев С. П., Павлов І. М. Математична модель захисту інформації в автоматизованих мережах спеціального призначення // Збірник наукових праць ВІТІ НТУУ „КПІ”. – К.: ВІТІ НТУУ „КПІ”. – 2004. – Вип. 5. – С. 147-153.* ***5.*** *Подиновский В. В. Количественная важность критериев // Автоматика и телемеханіка. – 2000. – №5. – С. 110-123.* ***6****. Кононович В. Г., Голобородько Д. В. Методи та засоби захисту від несанкціонованого доступу в системі управління мережами електрозв'язку України // – К.: Зв'язок, № 2, 1999, с. 13-16.*

УДК 681.3:519.872

ПОСТАНОВКА ЗАДАЧИ ОПТИМАЛЬНОГО ВЫБОРА ФУНКЦИОНАЛЬНОГО ПРОФИЛЯ ЗАЩИЩЕННОСТИ

Анатолий Антонюк, Денис Берестов*, Сергей Пустовит*, Владимир Шилин**
Национальная академия государственной налоговой службы Украины
**ННДЦ оборонных технологий и военной безопасности Украины*
***Институт программных систем НАНУ*

Аннотация: **Рассмотрена постановка формальной задачи выбора оптимального профиля защищенности в автоматизированных системах. Детально описаны основные характеристики задачи.**
Summary: **The formal task to choice optimal profile of security in computer systems are considered. In details the common characteristics of the task are described.**
Ключевые слова: **Информационная система, защита информации, угроза, модель, ущерб, вероятность.**

I Введение

Как известно [1 – 4], процесс создания любой системы защиты информации (СЗИ) в защищенных автоматизированных системах (АС) включает обязательную процедуру выбора и последующей реализации стандартного функционального профиля защищенности (СФПЗ). В [3] приводится классификация АС и список из 90 СФПЗ. Таким образом, в задачу разработчика входит обследование свойств конкретной АС, как объекта защиты и выбор необходимого СФПЗ из данного списка. Там же отмечено, что в случае, когда ни один СФПЗ из данного списка не подходит к конкретной АС, разработчик должен создать свой, наиболее подходящий для него СФПЗ, обосновать и утвердить его.

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

В [6] предложена формальная постановка задачи синтеза оптимальной СЗИ, позволяющая определять наиболее рациональный вариант технической реализации СЗИ. Данный поход может быть использован для формулировки задачи выбора оптимального СФПЗ.

Напомним, что 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 полно обеспечивается защита от определенного вида угроз. Уровни услуг имеют иерархию по полноте защиты, хотя и не являются точными подмножествами друг

друга. Уровни начинаются с первого и возрастают до определенного значения n, где n – уникальное для каждого вида услуг число.

На современном уровне развития информационных технологий и с учетом конкретных требований и потребностей информационной безопасности в [1 – 4] определено всего 22 услуги. Они обеспечивают защиту от четырех основных типов угроз (угроз конфиденциальности, целостности, доступности и наблюдаемости).

Естественно, при создании защищенных АС у разработчика возникает вопрос: какие именно услуги и каких уровней следует принимать во внимание. Именно для этого в [4] все услуги разных уровней сгруппированы в определенные структуры – СФПЗ. 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 определенной логикой, требованиями, принципами и ограничениями. Очевидно, что в первую очередь учитывались такие сведения о АС, как ее класс и основные требования к защищаемой информации (преимущественное обеспечение конфиденциальности (К), целостности (Ц), доступности (Д), конфиденциальности и целостности (КЦ), конфиденциальности и доступности (КД), целостности и доступности (ЦД), конфиденциальности, целостности и доступности (КЦД)). Кроме того, принимались во внимание типы АС [4], уровень секретности обрабатываемой информации и другие показатели. При этом, однако, должен быть обеспечен определенный уровень защищенности, а затраты на СЗИ должны минимизироваться.

Таким образом, легко видеть, что СФПЗ является, по существу, вариантом технической реализации СЗИ. Ниже, развивая результаты [5 – 7], предлагается формальная постановка задачи выбора оптимального СФПЗ с использованием таких показателей как вероятность появления угроз, вероятность устранения угроз, предотвращенный ущерб за счет ликвидации угроз.

II Постановка задачи

Рассмотрим математическую модель СФПЗ. Пусть $\overline{P}$ – множество всех возможных СФПЗ. Под РЄ $\overline{P}$ 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 ИС воздействием угроз. Обозначим общий предотвращенный ущерб ИС через S(P).

Формальная постановка задачи имеет вид: найти

$$P_0 = \arg\max S(P), \quad P_0 \in \overline{P} \tag{1}$$

при ограничении

$$C(P_0) \le C_r .$$

Здесь P – некоторый вектор, характеризующий СФПЗ, $\overline{P}$ – множество допустимых профилей, P_0 – оптимальное значение вектора P, C_r – допустимые затраты на СФПЗ. Ниже рассматривается детализация показателя качества.

III Формализация основных понятий СЗИ

Вначале формально опишем такие основные понятия как СФПЗ, угроза и ущерб, наносимый информационной системе.

В соответствии с [8 – 9] каждая угроза информации является следствием реализации некоторого множества факторов, называемых дестабилизирующими (ДФ). Предположим, что злоумышленник (ЗЛ) имеет возможность реализовать некоторое множество ДФ, в результате чего может возникнуть множество угроз $t_i, i = 1,..., n$ (заметим, что n=4). Каждую i-ую угрозу будем характеризовать вероятностью ее появления P_{it} и ущербом, наносимым информационной системе $\mathbf{S}_{\text{i}}$.

Угрозы должны нейтрализоваться соответствующими средствами и механизмами СЗИ, которые обеспечиваются реализацией функциональных услуг. При этом основной характеристикой СЗИ будет вероятность устранения каждой i-ой угрозы P_{is}. Поскольку функциональные услуги составляют СФПЗ, то,

очевидно, что вероятность устранения 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. Разлагая в ряд до линейного члена данные функции, получим

$$P_{is} \approx g_i(0,...,0) + \sum_{j=1}^{m} \frac{\partial g_i}{\partial P_j} P_j .$$

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

$$P_{is} \approx \sum_{j=1}^{m} \frac{\partial g_i}{\partial P_j} P_j$$

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

$$0 \le \frac{\partial g_i}{\partial P_j} \le 1, \ \sum_{j=1}^{m} \frac{\partial g_j}{\partial P_j} = 1, i = 1, \ ..., n .$$

Их величины определяются экспертным путем. Экспертным путем определяются и все остальные компоненты вектора СФПЗ $P_i, i = 1, ..., m$.

За счет реализации необходимого СФПЗ обеспечивается уменьшение ущерба, наносимого ИС воздействием угроз. Обозначим общий предотвращенный ущерб ИС через S, а предотвращенный ущерб за счет ликвидации i-ой угрозы через r_i.

Предотвращенный ущерб выражается в, общем виде, соотношением:

$$S(P) = \sum_{j=1}^{n} P_j P_{jt} s_j .$$

Предотвращенный ущерб за счет ликвидации воздействия i-ой угрозы:

$$r_i = P_i P_{it} s_i .$$

Вероятность появления i-ой угрозы P_{it} определяется следующим образом. Как было указано ранее, каждая угроза зависит от вероятностей реализации некоторого множества дестабилизирующих факторов (ДФ) $D_i = \{d_{ij}, i = 1, ..., n_i\}$, т. е. $P_{it} = f_i(d_{i1}, ..., d_{in_i})$. Считая, что для каждого i=1, …, n указанные функции являются достаточно гладкими, получим их разложения в ряд (до линейных членов)

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

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

$$P_{it} \approx \sum_{j=1}^{n_i} \frac{\partial f_i}{\partial d_{ij}} d_{ij} ,$$

где каждая j-ая производная интерпретируется как степень влияния требования на вероятность устранения j-го ДФ (важность выполнения j-го требования для устранения j-го ДФ). При этом

$$0 \le \frac{\partial f_i}{\partial d_{ij}} \le 1, \ \sum_{j=1}^{n_i} \frac{\partial f_i}{\partial d_{ij}} = 1, \ \ i = 1, \ ..., n .$$

Вероятности появления d_{ij} j-го ДФ могут определяться статистически и практически соответствуют относительным частотам их появления

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

где λ_{ij} – частота появления j-го ДФ, а индекс i везде относится к соответствующему номеру угрозы. Величины производных определяются экспертным путем.

Ущерб, S_i, наносимый і-ой угрозой, может определяться в абсолютных единицах: экономических потерях, временных затратах, снижении уровня защищенности, объеме уничтоженной или испорченной информации и т. д. Здесь можно воспользоваться подходом из [6].

IV Выводы

В статье рассмотрена постановка формальной задачи оптимального выбора СФПЗ для защищенных АС, а также показаны возможности детального описания основных показателей, необходимых для этого – вероятность появления угроз, вероятность устранения угроз, предотвращенный ущерб за счет ликвидации угроз. Основными этапами решения этой задачи являются:

- сбор и обработка экспертной информации об угрозах – ущерб, частота появления;
- оценка стоимости СЗИ для конкретного СФПЗ, т. е. учет ограничения $C(P_0) \le C_г$.

Литература: ***1.*** *Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99. – Київ: ДСТСЗІ СБ України, 1999. – 16 с.* ***2.*** *Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2–004–99. – Київ: ДСТСЗІ СБ України, 1999. – 55 с.* ***3.*** *Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2. 2–005–99. – Київ: ДСТСЗІ СБ України, 1999. – 23 с.* ***4.*** *Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99. – Київ: ДСТСЗІ СБ України, 1999. – 26 с.* ***5.*** *Антонюк А., Берестов Д. С., Пустовіт С. М. Аналіз складу профілів захищеності інформації Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2005. - №10. – 46-51 С.* ***6.*** *Кудин Д., Корольков В. Количественные оценки качества функционирования системы защиты информации // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2005. – №6. – 35-37 С.* ***7.*** *Антонюк А., Жора В. Моделювання доступу та каналів витоку в інформаційних системах /Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. - №3. – 156-160 С.* ***8.*** *Герасименко В. А. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат.-1994.-тт.1, 2.* ***9****. А. А. Антонюк, Е. Н. Боровская, В. Ю. Суслов Модель угроз информации в защищенных автоматизированных системах // Безопасность информации. – № 2. – 2001. – 25-28 С.*

УДК 681.3:519.872

ОБОБЩЕНИЕ МОДЕЛИ УГРОЗ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ

Анатолий Антонюк, Виктор Жора*
Академия ГНС Украины
**Институт программных систем НАНУ*

Аннотация: **Рассматриваются вопросы построения модели угроз в информационно-телекоммуникационной системе. Предлагается определение и классификация компонентов модели угроз, а также типовые алгоритмы реализации угроз. Приводится пример обобщенной модели угроз в информационно-телекоммуникационной системе.**

Summary: **The issues of developing threat model in information and telecommunication system are considered. Determination and classification of threat model components as well as typical algorithms of threat realization are offered. The example of generalized threat model in information and telecommunication system is given.**

Ключевые слова: **Информационно-телекоммуникационная система, угроза, атака, уязвимость, дестабилизирующий фактор.**

I Введение

Анализ угроз информации является одним из важнейших этапов при разработке комплексных систем защиты информации (КСЗИ) в информационно-телекоммуникационных системах (ИТС) и проводится на основании предварительно разработанной модели угроз. Согласно [1], модель угроз – это абстракное формализованное или неформализованное описание методов и способов осуществления угроз. На основании модели угроз также формируется политика безопасности (ПБ), в которой находят отражение