УДК 004.05

Игнатов В. А., д-р техн. наук,
Гузий Н. Н., канд. техн. наук

ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Институт компьютерных технологий Национального авиационного университета

В работе показано, что существуют необходимые и достаточные условия для построения систем оптимального управления информационной безопасностью. Доказана теорема об оптимальном значении стоимости ресурсов, необходимых для обеспечения заданного уровня информационной безопасности. Принятие решения относительно выбора ресурсов защиты сведено к типовой задаче поиска экстремума функции одной переменной. Практическую значимость утверждений теоремы подчеркивают три следствия, которые играют роль практических рекомендаций.

Введение. Обеспечение информационной безопасности в условиях противоборства информационных систем (ИС) является важной и актуальной задачей. Особого внимания заслуживает поиск таких методов и средств защиты, которые обеспечивают оптимальное использование ограниченных ресурсов.

Анализ проблемы. В соответствии с [1], под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры. На практике важнейшими являются три аспекта информационной безопасности – доступность, целостность и конфиденциальность. Обеспечение режима информационной безопасности – комплексная задача, которая должна учитывать особенности современных информационных систем: глобальную связанность и разнородность корпоративных систем, распространение технологии клиент/сервер.

В общем случае взаимодействие различных ИС можно классифицировать по соотношению критериев их эффективности (повышение эффективности – "содействие"; снижение – "противодействие", "конфликт").

Конфликт – системное явление, необходимо анализировать его структурные, вероятностные, динамические и теоретико-игровые свойства. Конфликт можно рассматривать как систему, включающую в качестве подсистем противоборствующие стороны со множеством связей, решающие задачу достижения некоторой цели. В конфликте могут участвовать несколько систем. Информационная борьба в этом случае должна рассматриваться как процесс взаимного воздействия друг на друга подсистем противоборствующих ИС.

Одной из основных задач, решаемых в ходе конфликта, является выбор альтернативы поведения ИС в соответствовии со стратегиями сторон, соотношению сил и ресурсов (оптимизация отношения «стоимость ресурсов защиты / потери от нарушения защиты») [2]. Информационный ресурс – это количественные и качественные характеристики ресурсов ИС. Понятие ресурсов включает все компоненты ИС (информация в ИС; аппаратное и программное обеспечение; процедуры, протоколы, управляющие структуры и т. п). Под интеллектуальным ресурсом понимается способность ИС функционировать в соответствии с поставленной целью и адаптироваться к изменяющейся среде конфликта [3].

Для реализации интегрированной системы защиты информации (СЗИ) необ-

ходимо определить информацию, подлежащую защите в ИС, выявить возможные каналы утечки, призвести оценку уязвимости информации, разработать политику безопасности, осуществить выбор средств и методов защиты, внедрить систему и обеспечить управление системой защиты.

Моделирование риска при создании и эксплуатации СЗИ осуществляется на основе функциональных зависимостей между риском, стоимостью СЗИ, вероятностью преодоления СЗИ и нанесения ущерба и размером возникающего при этом ущерба. Наиболее разработанным инструментом моделиравания взаимодействия ИС является математическая теория игр и методы оптимизации [4]. Анализ функционирования СЗИ и определения показателей эффективности системы в условиях противодействия приводят к разработке математических моделей и методик, основанных на имитационном моделировании. Для практических приложений целесообразно рассмотреть упрощенные методики управления информационной безопасностью.

Цель работы – построение математических моделей и доказательство фундаментальной теоремы о существовании необходимых и достаточных условий для оптимального управления ресурсами защиты для обеспечения требуемого уровня информационной безопасности в условиях преднамеренных деструктивных воздействий на ИС.

Постановка задачи. Предполагаются известными функции нападения и защиты по всем возможным видам атак и защит, а также ограничения на те или иные виды ресурсов, которые, как правило, имеют место при решении типовых задач обеспечения информационной безопасности. Методами математического программирования, прикладной математики, теории случайных функций требуется определить необходимые и достаточные условия существования и единственности оптимального управления информационной безопасностью.

Решение задачи. Обозначим через $N_1(r)$, $N_2(r)$, соответственно, зависимости числа методов нападения N_1 и защиты N_2 от стоимости r ограниченных ресурсов, используемых для нападения и защиты. Воспользуемся линейным приближением функций $N_1(r)$ и $N_2(r)$, для чего разложим их в ряд Тейлора с удержанием первых двух членов ряда, получим систему уравнений нападения и защиты вида

$$\begin{cases} N_1(r) = N_{1\,max} - \dfrac{\partial N_1(r)}{\partial r}(r - r_1), \\ N_2(r) = N_{2\,max} + \dfrac{\partial N_2(r)}{\partial r}(r - r_2), \end{cases} \qquad (1)$$

где через $N_{1\,max}$, $N_{2\,max}$, соответственно, обозначены максимальные значения числа методов, $\dfrac{\partial N_1(r)}{\partial r}$, $\dfrac{\partial N_2(r)}{\partial r}$ – производные функций $N_1(r)$, $N_2(r)$, r_1, r_2 – границы интервала стоимостей r используемых ресурсов, $r \in [r_1, r_2]$.

Равновесная стоимость r_0 используемых ресурсов определяется из уравнения «баланса числа методов нападения и защиты»

$$N_1(r_0) = N_2(r_0). \qquad (2)$$

Разрешая это уравнение относительно r_0, с учетом системы (1), получим

$$r_0 = \frac{N_{1\max} - N_{2\max} + N_1'(r)r_1 + N_2'(r)r_2}{N_1'(r) + N_2'(r)}, \qquad (3)$$

где для упрощения записи введены сокращенные обозначения производных в виде

$$\frac{\partial N_1(r)}{\partial r} = N_1'(r), \quad \frac{\partial N_2(r)}{\partial r} = N_2'(r).$$

Подставляя значение r_0 в уравнения системы (1), нетрудно определить число методов нападения и защиты, которые могут быть разработаны на ограниченные ресурсы, стоимостью r_0.

$$N_1(r_0) = N_{1\,max} - \frac{N_1'(r_0)}{N_1'(r_0)+N_2'(r_0)}[N_{max} - N_{2\,max} + N_2'(r_0)\,(r_2 - r_1)], \quad (4)$$

$$N_2(r_0 = N_{2\,ma} + \frac{N_2'(r_0)}{N_1'(r_0)+N_2'(r_0)}[N_{1\,max} - N_{2\,max} - N_1'(r_0)\,(r_2 - r_1)]. \quad (5)$$

Анализ системы уравнений (4), (5) позволяет получить качественную иллюстрацию «баланса методов нападения и защиты» (рис. 1).

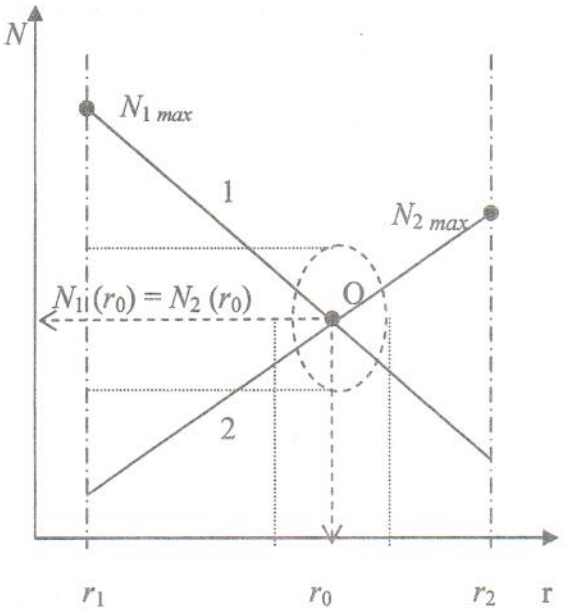

Рис. 1. Иллюстрация "баланса методов нападения и защиты"

Теорема об оптимальном управлении информационной безопасностью.

Если:

1. Методы нападения и защиты описываются системой уравнений (1),

2. Стоимость r_0 используемых ресурсов определяется из уравнения «баланса числа методов нападения и защиты» (2),

3. Уравнение (2) рассматривается как уравнение оптимизации стоимости ресурсов из условия «баланса числа методов нападения и защиты»,

то значение стоимости r_0 используемых ресурсов является оптимальным r_{opt} по критерию максимального правдоподобия, представленному в виде следующей целевой функции

$$\Phi(r, r_0) = r^2 - 2*r*\frac{N_{1\max} - N_{2\max} + N_1'(r_0)r_1 + N_2'(r_0)r_2}{N_1'(r_0)+N_2'(r_0)} - \frac{2C}{N_1'(r_0)+N_2'(r_0)}, \quad (6)$$

где постоянная интегрирования C определяется уравнением

$$C = -\frac{[N_{1\max} - N_{2\max} + N_1'(r_0)r_1 + N_2'(r_0)r_2]^2}{2[N_1'(r_0)+N_2'(r_0)]} \quad (7)$$

Доказательство теоремы выполнено с использованием результатов работ [5, 6, 7]. Из теоремы вытекают три практически важных следствия:

Следствие 1. Для определения оптимальной стоимости $r_0 = r_{opt}$ ресурсов нападения и защиты необходимо проводить исследования числа возможных методов нападения и защиты для нахождения зависимостей (1).

Следствие 2. Так как параметры зависимостей (1) неизбежно оцениваются с погрешностями, необходимо оценивать то, как эти погрешности влияют на оценивание оптимальной стоимости ресурсов, а также на результаты оценивания всех других функций r_{opt}.

Следствие 3. Чтобы $r_{opt} \in [r_1, r_2]$, необходимо выполнение следующих условий

$$\begin{cases} N_1'(r_0) \geq \dfrac{N_{1\max} - N_{2\max}}{2 - r_1}, \\ N_2'(r_0) \leq \dfrac{N_{1\max} - N_{2\max}}{r_2 - r_1}, \\ N_1'(r_0) > N_2'(r_0). \end{cases} \quad (8)$$

На рис. 2 показаны графики зависимостей критерия оптимальности $\Phi(r, r_0)$ при отсутствии погрешностей исходных данных (кривая 1) и для случая, когда существуют такие погрешности (кривая 2), σ_ϕ – минимальная среднеквадратическая погрешность.

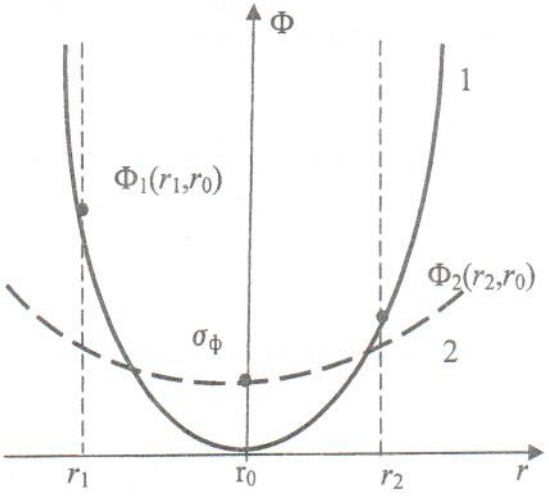

Рис. 2. Иллюстрация оптимальности используемых ресурсов

Выводы

1. Рассмотрение возможностей оптимального управления информационной безопасностью с точки зрения обеспечения динамического равновесия (баланса) числа метод нападения и защиты является перспективным направлением развития теории и практики обеспечения информационной безопасности.

2. Теорема об оптимальной стоимости используемых для защиты ресурсов – об оптимальном управлении информационной безопасностью – определяет необходимые и достаточные условия поиска оптимальных решений.

3. Практическую значимость утверждений теоремы подчеркивают три ее следствия, которые играют роль практических рекомендаций для разработки способов оптимального управления информационной безопасностью.

Список литературы

1. *Галактенко В. А.* Основы информационной безопасности. – М.: Интернет-Университет ИТ, 2004. – 264 с.

2. *Черней Г. А., Охрименко С. А., Ляху Ф. С.* Безопасность автоматизированных информационных систем. – Кишинев: Ruxanda, 1996. – 186 с.

3. *www.kiev-security.org.ua.*

4. *Гермейер Ю. Б.* Игры с противоположными интересами. – М.: Наука, 1976.

5. *Игнатов В. А., Гузий Н. Н.* Оптимальное управление скаляризацией векторных критериев в конфликтующих системах / Проблеми інформатизації і управління: Зб. наук. праць. – К.: НАУ, 2004. – №11. – С. 118-126.

6. *Игнатов В. А., Минаев Ю. Н., Гузий Н. Н.* Асимптотическая теория математического моделирования критериев оптимальности и ограничений / Захист інформації: Зб. наук. праць. – К.: НАУ, 2004. – №4. – С. 47-55.

7. *Игнатов В. А., Гузий Н. Н.* Метод ранжирования и цензурирования показателей качества функционирования сложных систем / Захист інформації: Зб. наук. праць. – К.: НАУ, 2004. – №3. – С. 83-93.