УДК 004.056

Б.Н. Епифанцев, А.А. Шелупанов, Е.Б. Белов

Подход к оптимизации ресурсов для защиты информации в организационных системах*

Сформулирован подход к оценке степени защиты информации в организационных системах при минимуме суммы затрат на ее создание и ущерба, наносимого пропущенными атаками.

Ключевые слова: защита информации, экономический критерий, оптимальность.

Случаи обеспечения стопроцентной защиты информационных ресурсов предприятия регламентируются руководящими документами ФСТЭК [1]. Когда их положения носят рекомендательный характер, неизбежно встает вопрос о величине расходов по статье «информационная безопасность». Обозначилась задача о создании некой системы формализованных правил, позволяющей внести элемент обоснованности в принимаемые решения. Возможный подход к решению такой задачи рассмотрен ниже.

В основу предлагаемого подхода положим экономический критерий. Известно, что при наличии в системе противодействующих факторов минимум расходов на поддержание ее функционирования дает определенное соотношение этих факторов. Обозначенное положение применительно к рассматриваемому вопросу иллюстрирует рис. 1. Ось ординат – расходы, которые несет хозяйствующий субъект при наличии у него информационного ресурса (кривая *3*). Они складываются из расходов, направляемых на защиту этого ресурса (кривая *2*) и потерь от внешних и внутренних атак, завершившихся успешно (кривая *1*). Ось абсцисс отражает степень защиты информационных ресурсов, измеряемая в диапазоне 0–100% или 0–1.

Точка минимума определяет рациональный уровень защиты прикрываемых сведений от внешних и внутренних атак при использовании экономического критерия. Степень защиты: $I = f(N_2, \alpha, \beta)$ есть функция числа защитников N_2, их квалификации α и уровня используемых программно-аппаратных средств β.

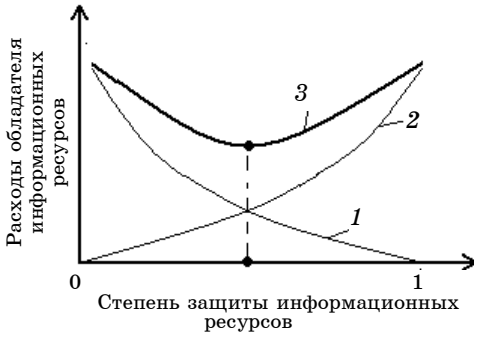

Рис. 1. Иллюстрация рационального принципа защиты информации по экономическому критерию

В [2] приведено уравнение прироста успешных атак на ресурсы организации. В обобщенном варианте его можно представить в виде

$$\frac{dN_1(t)}{dt} = \left[\kappa_1\left(\frac{D}{p}\right)\cdot N_1(t) - \kappa_2\left(\frac{\Pi_{90}}{\Pi}\right)N_1(t)\right](1-I), \quad (1)$$

где D/p – отношение среднего дохода правонарушителя от проведенной операции к расходу на ее проведение; Π_{90}/Π – отношение уровня преступности в стране в 90 г. к текущему уровню преступности. Функция $\kappa_1(D/p)$ характеризует степень «алчности» членов сообщества – долю населения, готовую пойти на правонарушение в зависимости от ожидаемого дохода и имеющую достаточный уровень квалификации для совершения преступления в рассматриваемой сфере интеллектуальной деятельности. Для разных сообществ вид зависимости $\kappa_1(D/p)$ описывается логистической кривой

$$\kappa_1(D/p) = a_n / \left[1 + b\cdot\exp(-c\cdot D/p)\right],$$

где коэффициент a_n определяется уровнем культуры («нравственного здоровья») и грамотностью населения, b и c – коэффициенты. Для слаборазвитых сообществ $a_n \geq 0{,}15$, аб-

* Работа выполнена в рамках реализации программы «Научные и научно-педагогические кадры инновационной России на 2009–2013 годы», контракт № П215 от 22.07.09 г.

цисса точки пересечения кривой с уровнем a_n определяется экспертными технологиями. Что касается уровня «нравственного здоровья» населения, его оценку дают аналитические отделы разведслужб. В открытой литературе для этих целей используется так называемый «индексный метод объединения разнородных показателей». Число таких показателей доходит до 40: душевое потребление алкоголя, количество убийц и суицидов, посещаемость населением музеев и т.д. Вариант кривой $\kappa_1(D/p)$ приведен на рис. 2.

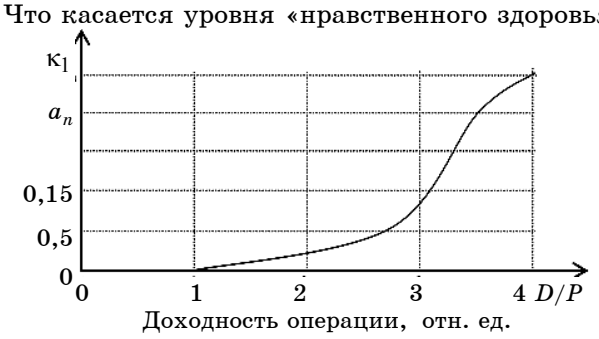

Рис. 2. Вариант поведения функции $\kappa_1(D/p)$

О влиянии грамотности населения на уровень a_n дает представление график на рис. 3а.

Функция $\kappa_2(\Pi_{90}/\Pi)$ отражает законопослушность населения через приращение преступности относительно ее значения в определенном (опорном) году.

При $(\Pi_{90}/\Pi)\to 0$ $\kappa_2(\ldots)\to 0$,

при $(\Pi_{90}/\Pi)=1$

$dN_1/dt=0$ и $\kappa_2(\Pi_{90}/\Pi)=\kappa_1(D/p)$.

Функция $\kappa_2(\Pi_{90}/\Pi)$ – нелинейная (следует из рис. 3б).

В небольших диапазонах изменения преступности П ее можно представить в виде

$$\kappa_2(\Pi_{90}/\Pi)=(\Pi_{90}/\Pi)\cdot\kappa_1(D/p).$$

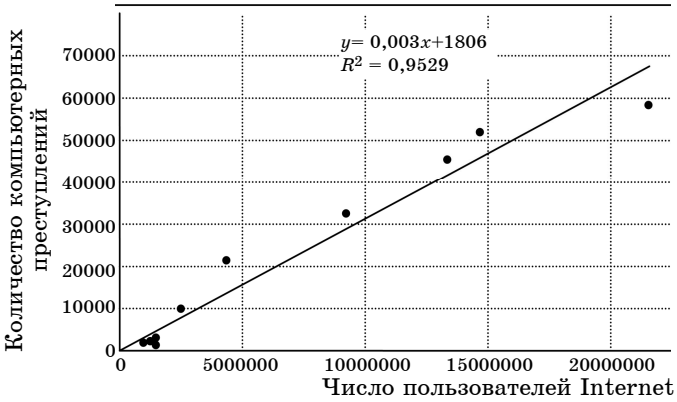

Рис. 3а. Зависимость числа компьютерных преступлений от числа пользователей Internet

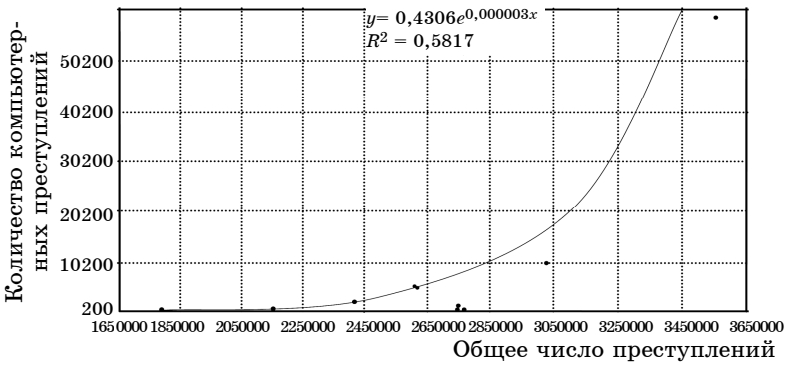

Рис. 3б. Зависимость числа компьютерных преступлений от общего числа преступлений в стране

Определимся с функцией $I=f(N_2,\alpha,\beta)$ в (1). При высшей степени защиты I =1 атаки не проходят: (dN_1/dt)=0 ущерб $У$ минимальный, расходы на защиту P максимальны, $(У/P)\cong 0$. Другую точку кривой $(I=0,(У/P)=?)$ можно оценить из следующих соображений. Обратимся к простейшей модели сражения Ланкастера, описывающей борьбу двух противостоящих сил. Из её анализа следует: для борьбы с вдвое более многочисленным противником необходимо для его уничтожения иметь в четыре раза более мощное оружие, с втрое более многочисленным противником – в девять раз и т.д.

Модель сражения позволяет построить функцию $I=f(У/P)$ и на ней получить значение I (1) в точке, обеспечивающей искомый минимум на кривой 3 (см. рис. 1). Связь между I (1) $=f(N_2,\alpha,\beta)$, позволяющая при заданных I (1) и β оценить соотношение «количество защитников – их качество», обсуждена в [3].

Таким образом, последовательность действий и их содержание для обеспечения минимальных затрат на защиту информационного ресурса обсуждено с необходимой степенью подробности. В следующем сообщении планируется обсудить количественные оценки эффективности использования рассмотренного подхода при решении типовых задач по обеспечению безопасности информационных ресурсов организации.

Литература

1. Белов Е.Б. Основы информационной безопасности / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М. : Горячая линия – Телеком, 2006. – 544 с.
2. Епифанцев Б.Н. Борьба с инсайдерскими угрозами: системный подход // Докл. Том. гос. ун-та систем управления и радиоэлектроники. – 2008. – № 2 (18), ч 1. – С. 73–74.
3. Епифанцев Б.Н. Состояние и перспективы подготовки и повышения квалификации кадров в сфере информационной безопасности в регионе // Безопасность и банковский бизнес: матер. межрегион. науч.-практ. конф. 22 ноября 2007 г. – Омск: Издательский комплекс «ГЭПИЦЕНТР–II», 2007. – С. 46–53.

Епифанцев Борис Николаевич
Доктор техн. наук, профессор, зав. каф. информационной безопасности
Сибирской гос. автомобильно-дорожной академии (СибАДИ), г. Омск
Тел.: (3812) 25-04-80
Эл. почта: epifancev_bn@sibadi.org

Шелупанов Александр Александрович
Доктор техн. наук, профессор, проректор по научной работе ТУСУРа
Тел.: (382-2) 51-05-30
Эл. адрес: office@udcs.ru

Белов Евгений Борисович
Сотрудник ИКСИ Академии ФСБ, г. Москва,
Тел.: (495) 931-06-09
Эл. адрес: umo@academy.fsb.ru

B.N. Epifancev, A.A. Shelupanov, E.B. Belov

The approach to optimization of resources for information protection in organizational systems

The approach to an estimation of degree of protection of the information in organizatsionnyh systems is formulated at a minimum of the sum of expenses for its creation and the damage put by passed attacks. Approach and criteria risk of information security.
Keywords: information protection, economic criterion, optimality information security, risk, identification.