Г.Е. Шепитько
(Московская финансово-юридическая академия;
e-mail: ge2004@yandex.ru)

ИДЕНТИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ОБЪЕКТОВ ОТ ВНУТРЕННИХ НАРУШИТЕЛЕЙ

Аннотация. Обосновано третье уравнение безопасности объектов при посягательстве на них внутренних нарушителей различных категорий подготовленности. Получены аналитические оценки для вероятностей попыток совершения инцидентов и вероятностей замыслов этих попыток для различных категорий важности объектов.

Ключевые слова: уравнение безопасности, инцидент, категории подготовленности внутренних нарушителей, категории важности объектов, попытки совершения инцидента, замыслы совершения попыток, потенциальный, начальный и остаточный уровень угроз безопасности.

G.E. Shepitko

IDENTIFICATION OF INSIDERS SECURITY THREATS TO OBJECTS

Abstract. The third equation of object's security at their encroachment on insiders various categories of preparedness is proved. Analytical estimates for the probability of attempted incidents and the probability of these plans attempt for different categories of the object's importance are got.

Key words: equation of safety, incident, insider's categories of preparedness, categories of the object's importance, attempted incidents, plans attempt, potential, base and residual level security threats.

Статья поступила в редакцию Интернет-журнала 26 августа 2010 г.

В работе [1] получено второе уравнение безопасности важного объекта, на который посягается один внутренний нарушитель с заданным уровнем подготовленности. Однако, реальный объект привлекает несколько типов нарушителей различной степени подготовленности.

Целью данной статьи является оценка предельных значений угроз безопасности объектов различных категорий важности, на которые посягаются несколько типов нарушителей различной подготовленности.

Для корректности постановки задачи примем следующие допущения. На объекте установлено N предметов защиты, M объектов защиты относятся к одной из категорий важности (КТ4 – простой объект, КТ3 – важный, КТ2 – особо важный, КТ1 – особо важный объект с повышенной значимостью ценностей) [3]. На объект защиты посягаются с разной вероятностью внутренние нарушители различной степени подготовленности (СЛ – случайный нарушитель, ПН – подготовленный нарушитель, КВ – квалифицированный нарушитель, ВК – высококвалифицированный нарушитель) [2].

Известны статистические данные об интенсивности инцидентов, совершённых нарушителями различных категорий подготовленности на объектах различной категории важности. Необходимо обосновать математическую модель защиты объектов для идентификации уровней потенциальных и начальных угроз безопасности этих объектов. Согласно [4] для разрешения проблемы идентификации угроз надо решить обратную задачу: при известных выходных воздействиях "серого ящика" найти входные воздействия.

При балансе разведок системы защиты и нарушителей в части обоснования структуры защиты объекта имеет место следующая теорема.

Теорема. При воздействии пуассоновского потока инцидентов нескольких внутренних нарушителей различных категорий подготовленности с переменным ресурсом, поведение автономной линейной системы безопасности первого порядка с переменными параметрами описывается третьим уравнением безопасности:

$$P(T) = \exp\{ -\lambda c\ T\}, \qquad (1)$$

где $P(T)$ – вероятность отсутствия инцидентов за время T;

λc – суммарное значение интенсивности инцидентов от всех типов внутренних нарушителей;

$$\lambda c = \sum_{i=1}^{4} \lambda i; \qquad (2)$$

λi – интенсивность инцидентов по вине нарушителя i-й категории подготовленности;

$$\lambda i = \lambda_0\ K_{1i}\ K_{2i}\ K_{3i}; \qquad (3)$$

λ_0 – начальное значение интенсивности инцидентов;

$K_{1i} = d_i$ – доля нарушителей i-й категории подготовленности среди внутренних нарушителей;

K_{2i} – коэффициент замыслов попытки совершения инцидента нарушителем i-й категории подготовленности;

$$K_{2i} = \exp[-\ a_0\ \boldsymbol{q}\ \exp(-\ \alpha_i\ \boldsymbol{q})]; \qquad (4)$$

K_{3i} – коэффициент попыток совершения инцидента нарушителем i-й категории подготовленности;

$$K_{3i} = \exp[-\ a - b_0\ (1+\ b_1\ (\boldsymbol{q}\ -1))\ (\boldsymbol{q}-1)\ \exp(-\alpha_i\ \boldsymbol{q})]; \qquad (5)$$

$\boldsymbol{q}$ – количество рубежей защиты объекта (показатель объёма ресурсов защиты);

α_i – нормативы амортизации ресурсов системы предупреждения и системы защиты объекта из-за их морального старения;

a, a_0, b_0, b_1 – постоянные коэффициенты.

Доказательство

С учётом 4-х типов нарушителей математическая модель защиты объекта описывается системой из четырёх независимых дифференциальных уравнений первого порядка, решение Коши которой на основе результатов [1] для i=1, 2, 3, 4 имеет вид

$$\lambda i = \lambda_0 \exp\text{-}[a + \ln d_i + \{a_0 \boldsymbol{q} + b_0 (1 + b_1 (\boldsymbol{q} - 1)) (\boldsymbol{q} - 1)\} \exp(-\alpha_i \boldsymbol{q})], \quad (6)$$

где из условия баланса разведок $\alpha = \beta = \gamma$ и для компактности записи приняты значение параметров $a_1 = A_0 = X_0 = 1$, $T = 1$ год.

Путём перестановки слагаемых в показателе (6), это решение можно представить в мультипликативной форме:

$$\lambda i = \lambda_0 * \exp[\ln d_i] * \exp[-a_0 \boldsymbol{q} \exp(-\alpha_i \boldsymbol{q})] \cdot$$
$$\cdot \exp[-a - b_0 (1 + b_1 (\boldsymbol{q} - 1)) (\boldsymbol{q} - 1) \exp(-\alpha_i \boldsymbol{q})] \quad (7)$$

из которого следуют искомые выражения (3-1).

Для идентификации уровня угроз безопасности объекта необходимо выполнить калибровку параметров системы предупреждения и системы защиты объекта.

На основании опыта физической защиты объектов известны диапазоны вероятностей защиты $P_{защ}i$ = 0,9-0,95 и предупреждения $P_{пред}i$ = 0,2-0,5 инцидентов внутренних нарушителей [4]. Тогда могут быть найдены искомые значения доли нарушителей d_i из следующего условия:

$$\lambda i\{d_i, P_{защ}i, P_{пред}i, \alpha_i, \boldsymbol{q}\} = \lambda icp(\boldsymbol{q}_{эксп}), \quad (8)$$

где λi { } – теоретическое значение интенсивности инцидентов по вине нарушителя i-й категории подготовленности, которое определяется расчётным путём по формуле (3);

α_i – норматив амортизации систем из-за морального старения;

$\lambda icp(\boldsymbol{q}_{эксп})$ – экспериментальное значение интенсивности инцидентов по вине нарушителя i–й категории подготовленности, которое определяется методом наименьших квадратов при выполнении равенства

$$\boldsymbol{q}_{эксп} = 5 - Km; \quad (14)$$

Km – номер категории важности объекта [1].

С целью экспериментальной проверки возможности оценки уровней угроз безопасности реальных объектов были собраны статистические данные о 30 объектах информатизации, содержащих коммерческую тайну (количество предметов защиты – рабочих станций N = 3000, количество компьютерных нарушений K = 500, период наблюдения T = 1 год). При проведении расчётов приняты значения параметров $\lambda_0 = a = 0{,}78$; $a_0 = b_0 = b_1 = 0{,}5$. В результате получены значения норматива амортизации α_i = {0,15; 0,25; 0,37; 0,5} и доли нарушителей d_i = {0,8; 0,15; 0,04; 0,01} соответственно для случайного, подготовленного, квалифицированного и высоко квалифицированного нарушителя.

На рис. 1 представлены зависимости интенсивностей замыслов, попыток и инцидентов от отношения ресурсов $\boldsymbol{q}$, из рассмотрения которых следует, что увеличение ресурсов защиты не позволяет существенно снизить количество инцидентов квалифицированного нарушителя вследствие опережающего роста вероятности обхода им системы защиты объекта.

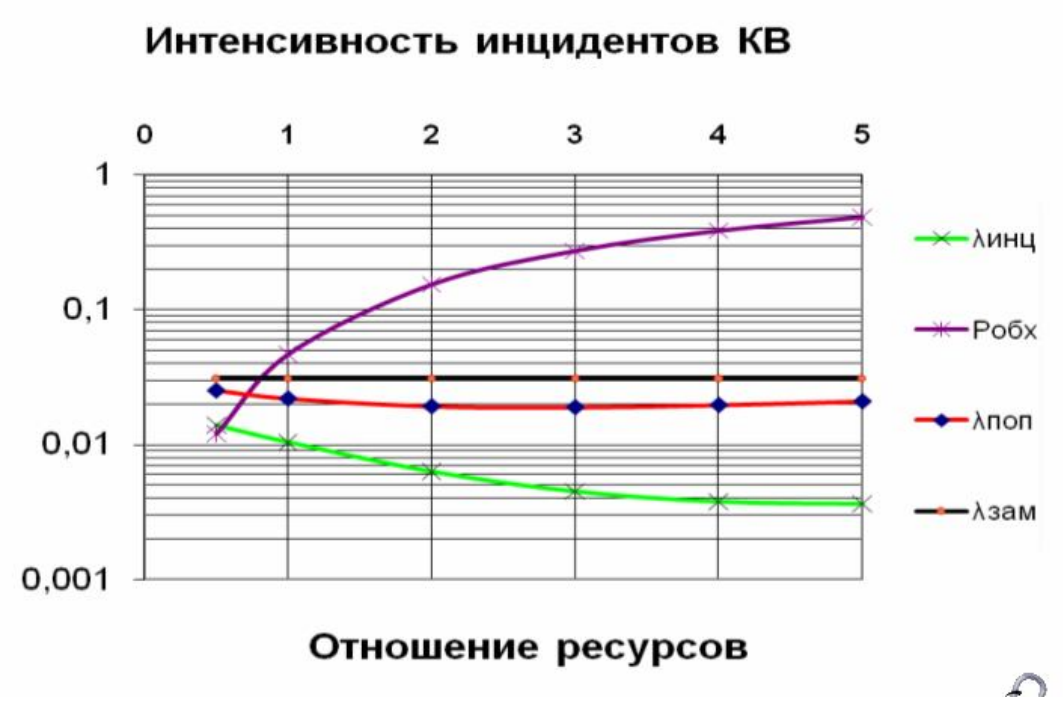

Рис. 1. Зависимости интенсивностей замыслов, попыток и инцидентов от отношения ресурсов

На рис. 2 представлены зависимости суммарных значений интенсивностей замыслов, попыток и инцидентов от номера категории важности объекта для внутренних нарушителей.

Рис. 2. Зависимости суммарных значений интенсивностей замыслов, попыток и инцидентов от категории важности объекта

Из рассмотрения этих зависимостей следует, что количество попыток на один инцидент находится в пределах 2-10, количество замыслов на одну попытку в интервале 1-2, что соответствует экспертным оценкам криминалистов.

Изложенный подход к оценке уровней угроз безопасности объектов может быть полезен при решении задач мониторинга уровня интенсивности криминогенной обстановки на региональном уровне.

Вывод. Впервые выявлена теоретически и экспериментально подтверждена возможность оценки потенциального и начального уровней угроз безопасности объектов от внутренних нарушителей.

Литература

1. **Шепитько Г.Е.** Потенциальная безопасность объекта при переменном ресурсе внутреннего нарушителя // Технологии техносферной безопасности: Интернет-журнал. – Вып. 4 (26). – 2009. – 7 с. – http://ipb.mos.ru/ttb/2009-4/2009-4.html. – 0420900050/0041.

2. **Шепитько Г.Е., Медведев И.И.** Проблемы безопасности объектов: учебное пособие. – М.: Академия экономической безопасности МВД РФ, 2006. – 192 с.

3. **Шепитько Г.Е.** Категорирование объектов информатизации // Материалы 16-й научно-технической конференции "Системы безопасности" – СБ-2008. – М.: Академия ГПС МЧС России, 2008. – С. 135-136. – http://ipb.mos.ru/sb/2008**.**

4. **Шепитько Г.Е.** Проблемы охранной безопасности объектов: монография. 2-е изд. – М.: АЭБ, 2010. – 208 с.