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

ПОТЕНЦИАЛЬНАЯ БЕЗОПАСНОСТЬ ОБЪЕКТА ПРИ ПЕРЕМЕННОМ РЕСУРСЕ ВНУТРЕННЕГО НАРУШИТЕЛЯ

Обосновано второе уравнение безопасности объекта. Приведены теоретические оценки интенсивности инцидентов и предельной вероятности защиты объекта от внутреннего преднамеренного квалифицированного нарушителя с переменным ресурсом.

Ключевые слова: потенциальная безопасность, второе уравнение безопасности, внутренний преднамеренный нарушитель, квалифицированный нарушитель, инсайдер, затраты на разведку, обход системы защиты.

G.E. Shepitko

THE POTENTIAL SECURITY OF THE FACILITY WITH A VARIABLE RESOURCE OF INTERNAL VIOLATOR

Proved the second equation of the security facility. The author gives theoretical estimates of the intensity of incidents and the limit probability of protecting the facility from the internal intentional qualified violator, with variable resource.

Key words: potential security, the second equation of the security, intentional internal violator, qualified Violator, insider, cost of exploration, bypassing the security system.

В работе [1] получено первое уравнение безопасности простого объекта, на который посягаются внутренние непреднамеренные нарушители с фиксированным ресурсом. Однако известно, что даже неподготовленные нарушители способны совершить обход системы защиты путём непреднамеренного или, тем более, преднамеренного невыполнения требований политики безопасности.

Целью данной статьи является оценка предельных значений системы безопасности важных объектов при противостоянии внутренним преднамеренным квалифицированным нарушителям с переменным ресурсом.

Для корректности постановки задачи примем следующие допущения. Объект защиты представляет собой совокупность большого числа N однородных предметов защиты и относится к ансамблю из M однородных объектов, на которых в течение периода времени T наблюдаются K случаев инцидентов безопасности, связанных с противоправными действиями внутренних нарушителей. Ансамбль объектов защиты относится к одной из категорий важности объектов $K_{\text{Т3}}$, $K_{\text{Т2}}$, $K_{\text{Т1}}$ [2], на которые чаще всего посягаются заранее подготовленные нарушители, способные совершенствовать свои приёмы нападения и совершать обход существующих средств защиты. Экономическая мощь системы защиты объекта и нарушителя ха-

рактеризуется объёмами их ресурсов A, V и X соответственно в виде стоимости ежегодных затрат в условных валютных единицах (уве). Инциденты безопасности являются редкими событиями, поэтому выполняется неравенство $K \leq M\ N\ T$. С учётом принятой в [2] логарифмической шкалы оценки значений информативных признаков категорирования можно записать оценку степени важности объекта в виде

$$Q = 5 - K_{\text{Т}}, \qquad (1)$$

где $\text{К}_{\text{Т}}$ – номер категории важности объекта.

Тогда при повышении категории важности объекта от $K_{\text{Т4}}$ до $K_{\text{Т1}}$ степень важности объекта увеличивается от 1 до 4.

Из физических соображений представляется логичным, что при увеличении степени важности объекта Q должна увеличиться частота попыток нарушителя получить информацию о системе защиты объекта. Тогда имеет место следующее утверждение.

Утверждение 1

При воздействии пуассоновского потока инцидентов утечки информации о системе защиты объекта остаточная стоимость этой системы $\text{Ц}_{\text{мсз}}$ вследствие ускоренного морального износа описывается выражением:

$$\text{Ц}_{\text{мсз}} = \text{Ц}_{\text{сз}} \exp(-\mu\ Q\ T), \qquad (2)$$

где $\text{Ц}_{\text{сз}}$ – начальная стоимость системы защиты;

μ - норматив амортизации вследствие морального старения системы;

Q – степень важности объекта;

T – период времени наблюдения.

Для доказательства этого утверждения примем, что интенсивность потока $\lambda_{\text{уи}}$ инцидентов утечки информации (вследствие аналитической и разведывательной работы нарушителей) прямо пропорциональна степени важности Q защищаемого объекта:

$$\lambda_{\text{уи}} = \mu\ Q, \qquad (3)$$

тогда при пуассоновском потоке инцидентов вероятность одного и более инцидентов утечки информации за время T определяется формулой:

$$\text{Р}_{\text{уи}} = 1 - \exp(-\mu\ Q\ \text{Т}). \qquad (4)$$

Если информация о технических характеристиках, методах и тактике системы защиты составляет коммерческую тайну стоимостью $\text{Ц}_{\text{кт}}$, тогда стоимость разведывательной информации $\text{Ц}_{\text{ри}}$, полученной нарушителями, составит

$$\text{Ц}_{\text{ри}} = \text{Ц}_{\text{кт}} [1 - \exp(-\mu\ Q\ T)]. \qquad (5)$$

С другой стороны, утечка информации о системе защиты объекта приводит к ускоренному моральному старению этой системы:

$$\text{Ц}_{\text{мсз}} = \text{Ц}_{\text{сз}} \exp(-\Lambda\ T), \qquad (6)$$

где Λ – норматив ускоренной амортизации стоимости системы защиты вследствие морального старения.

Тогда разницу между $Ц_{сз}$ и $Ц_{мсз}$ можно трактовать как нанесённый нарушителями косвенный материальный ущерб системе защиты объекта:

$$У_{щ} = Ц_{сз} [1-\exp(-Λ T)], \quad (7)$$

Если стоимость информации характеризовать по последствиям её утечки в виде стоимости ущерба, тогда, приравнивая выражения (5) и (7), получим искомое выражение (2), что и требовалось доказать.

В частности, для вычислительной техники норматив ускоренной амортизации $\mu = 0{,}25$, тогда при $Q = 1 \div 4$ средний срок моральной службы $T_{мсл} = 1/(\mu\ Q)$ системы защиты составит от 4 до 1 года, что соответствует практике охраны объектов.

В реальности обе противостоящие стороны "система защиты" и "нарушитель" осуществляют разведку друг друга, из чего вытекает следующая теорема.

Теорема 2. При воздействии пуассоновского потока инцидентов внутренних преднамеренных нарушителей с переменным ресурсом поведение автономной линейной системы защиты первого порядка с переменными параметрами описывается вторым уравнением безопасности вида

$$P(T) = \exp\{-\lambda_0 T \exp[-(a_0 (1+a_1 (Q - 1)) A_0 \exp(- \alpha Q T) + + b_0 (1+ b_1 (Q - 1)) X_0 (q \exp(- \beta Q T) - \exp(- \gamma Q T))] T\}, \quad (8)$$

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

λ_0 – начальное значение интенсивности инцидентов;

$q = V/x$ - отношение стоимости $V\ T$ ресурсов системы защиты к стоимости $X\ T$ ресурсов нарушителя;

Q – степень важности объекта в смысле (1);

A_0, X_0 – начальные значения затрат в уве;

a_0, a_1, b_0, b_1, α, β, γ – постоянные коэффициенты.

Доказательство

В соответствии с первым уравнением безопасности [1] интенсивность инцидентов $Л(T)$ зависит только от отношения ресурсов q в виде:

$$\lambda(T) = \lambda_0 \exp[-(a A_0 + b (V_0 – X_0)] T, \quad (9)$$

$$V_0 = q X_0, \quad (10)$$

где a, b – постоянные коэффициенты;

q – количество одинаковых рубежей защиты объекта;

A_0, X_0 – начальные затраты системы безопасности на предупреждение инцидентов и начальные затраты нарушителей на совершение инцидентов соответственно. Для простых объектов (категория $K_{Т4}$) принимаются значения $A_0 = X_0 = 1$ уве.

Пусть для важных объектов значения коэффициентов a, b являются переменными и прямо пропорциональны степени важности объекта Q, тогда для ресурсов системы предупреждения, системы защиты и ресурсов

нарушителей для совершения нападения можно записать следующие соотношения:

$$A_1 = (1+a_1 (Q - 1)) A_0; \quad (11)$$

$$V_1 = (1+ b_1 (Q - 1)) X_0 q; \quad (12)$$

$$X_1 = (1+ b_1 (Q - 1)) X_0. \quad (13)$$

С учётом ускоренного морального износа ресурсов противоборствующих сторон получим на основе (2) и (11-13):

$$A = A_1 \exp(-\alpha Q T); \quad (14)$$

$$V = V_1 \exp(-\beta Q T); \quad (15)$$

$$X = X_1 \exp(-\gamma Q T), \quad (16)$$

где α, β, γ – нормативы амортизации ресурсов системы предупреждения, системы защиты и ресурсов нарушителей для совершения нападения соответственно.

Подставляя выражения (14-16) в соотношения

$$\lambda(T) = \lambda_0 \exp[-(a_0 A + b_0 (V - X)] T, \quad (17)$$

$$P(T) = \exp[-\lambda(T) T], \quad (18)$$

получим искомое второе уравнение безопасности, что и требовалось доказать.

Следствие 1

Если установить требование к количеству рубежей защиты в виде:

$$q = Q, \quad (19)$$

тогда можно найти значение $q_{опт}$, при котором будет достигнуто минимально возможное значение интенсивности инцидентов

$$q_{опт} = \arg \min_q \lambda(q, T) \quad (20)$$

На основе соотношения (18) можно записать выражения для вероятностей пропуска нарушителей при отсутствии и наличии разведывательных мероприятий с обеих сторон:

$$P(q) = 1 - \exp[-\lambda_1(q) T], \quad (21)$$

$$P(q, \alpha) = 1 - \exp[-\lambda_2(q, \alpha) T], \quad (22)$$

из которых следует выражение для вероятности обхода систем предупреждения и защиты нарушителями, приведённой к одному рубежу защиты:

$$P_{обх} = \sqrt[q]{1 - \exp[-\lambda_2 (q, \alpha) T]} - \sqrt[q]{1 - \exp[-\lambda_1 (q) T]}. \quad (23)$$

Для частного случая были проведены расчёты при $\lambda_0 = 0{,}4$, $a_0 = 0{,}3$, $a_1 = 1$, $b_0 = 0{,}5$, $b_1 = 0{,}5$, $\alpha = \beta = \gamma$, $A_0 = X_0 = 1$, $T = 1$ год.

На рис. 1 представлена зависимость предельной (максимально достижимой) интенсивности инцидентов нарушителей в зависимости от норматива амортизации α.

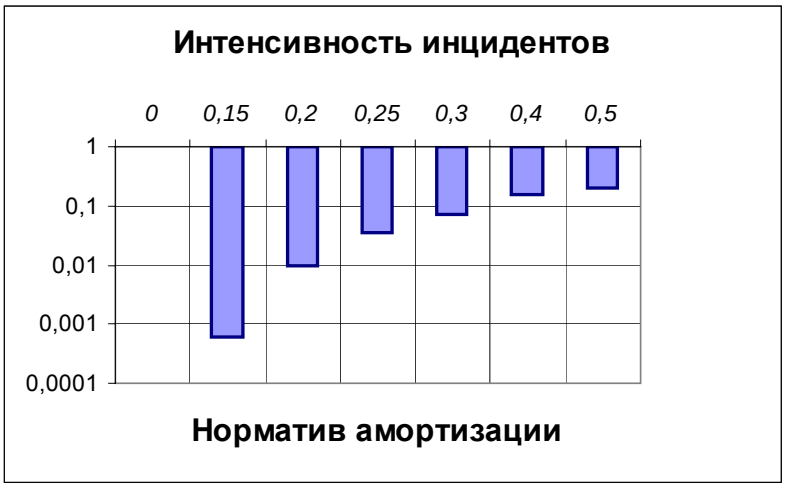

Рис. 1

Из рассмотрения этой зависимости следует, что снижение интенсивности инцидентов до 0,01 может быть достигнуто только при нормативе морального старения систем защиты не более 0,2 при балансе разведок обеих сторон.

На рис. 2 представлена зависимость вероятности обхода нарушителями систем предупреждения и защиты объекта от количества рубежей защиты, из которой следует, что для объекта категории $К_{Т1}$ при $q = Q = 4$ вероятность обхода достигает 0,25.

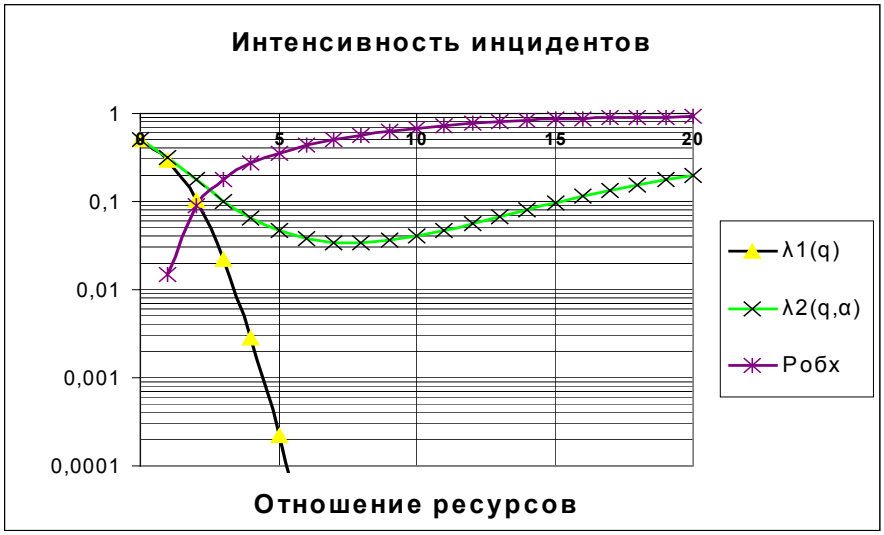

Рис. 2

Таким образом, при воздействии потока квалифицированных нарушителей предельная вероятность защиты объекта определяется не отношением физических ресурсов противоборствующих сторон, а степенью их информированности.

Следствие 2

Из выражений (5), (7) следует соотношение для стоимости разведывательной информации о системе защиты объекта:

$$Ц_{рсз} = Ц_{сз} [1 – \exp (-\beta Q T)]. \quad (24)$$

При этом саму разведывательную деятельность можно трактовать как специфическую НИОКР с нормативом окупаемости ε вложенных средств, тогда затраты нарушителей на изучение системы защиты объекта в первый год составят:

$$З_{нрсз} = Ц_{сз} [1 – \exp (-\beta Q T)] [1 – \exp (-\varepsilon T)]. \quad (25)$$

где ε = 0,15 – норматив окупаемости НИОКР [3].

$Ц_{сз}$ – стоимость системы защиты определяется по формуле:

$$Ц_{сз} = (1+ b_1 (Q – 1)) X_0 q. \quad (26)$$

Аналогичным образом определяются затраты нарушителей на разведку системы предупреждения и затраты системы защиты на разведку самих нарушителей:

$$З_{нрсп} = Ц_{сп} [1 – \exp (-\beta Q T)] [1 – \exp (-\varepsilon T)]; \quad (27)$$

$$З_{сзрн} = Ц_{сн} [1 – \exp (-\gamma Q T)] [1 – \exp (-\varepsilon T)]; \quad (28)$$

где

$$Ц_{сп} = (1+a_1 (Q – 1)) A_0; \quad (29)$$

$$Ц_{сн} = (1+ b_1 (Q – 1)) X_0. \quad (30)$$

В итоге можно определить полные расходы системы безопасности объекта, нарушителей и долю расходов нарушителей на разведку, а также стоимость материальных ценностей на объекте:

$$З_{сз} = (Ц_{сз} + Ц_{сп} + З_{сзрн}) N; \quad (31)$$

$$З_{нар} = (З_{нрсз} + З_{нрсп} + Ц_{сн}) N; \quad (32)$$

$$Д_{рир} = 100 (З_{нрсз} + З_{нрсп})/(З_{нрсз} + З_{нрсп} + Ц_{сн}); \quad (33)$$

$$Ц_{мц} = Ц_{сн} N/r, \quad (34)$$

где N – количество предметов защиты на объекте;

r – риск нарушителей при вложении средств на проведение инцидента.

В качестве примера рассмотрим защиту объекта информатизации в составе 30 рабочих станций пользователей с ценной коммерческой информацией. Для объектов категории $K_{Т4}$ стоимость станции составляет 500 \$, тогда при r =0,02 курс 1уве равен 10 \$. На рис. 3 представлены результаты расчёта затрат при $q = Q$, α = β = γ = 0,25,. ε = 0,15, N = 30, T = 1 год.

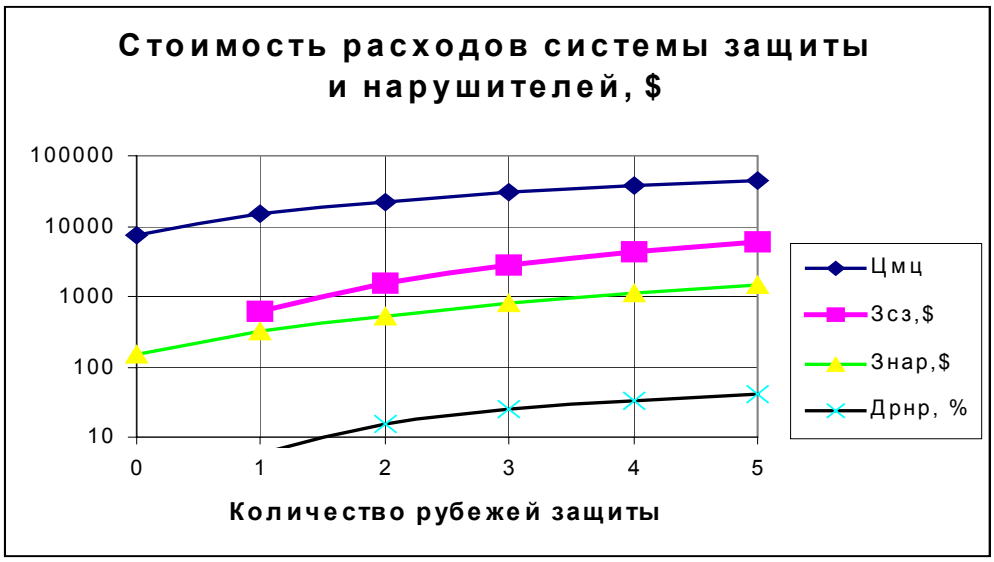

Рис. 3

Из рассмотрения полученных зависимостей следует, что при увеличении степени важности объекта с информацией, содержащей коммерческую тайну, существенно возрастает доля расходов нарушителей на разведывательные и аналитические мероприятия и превышает 50 %, что характерно для инсайдеров (высококвалифицированных внутренних нарушителей).

Вывод: потенциальная безопасность объекта при переменном ресурсе внутреннего нарушителя определяется степенью его информационного обеспечения о характеристиках системы защиты объекта.

Литература

1. Шепитько Г.Е. Аналитические оценки потенциальной безопасности объекта при фиксированном ресурсе внутреннего нарушителя / Интернет-журнал "Технологии техносферной безопасности" - № 3. - 2009. - http://ipb.mos.ru/ttb.

2. Шепитько Г.Е. Категорирование объектов информатизации // Семнадцатая научно-техническая конференция "Системы безопасности" - СБ-2008. – М.: Академия ГПС МЧС России, 2008. – С. 135-136.

3. Инструкция по определению экономической эффективности новой техники охранной и пожарной сигнализации, изобретений и рационализаторских предложений / Гудков А.В., Синилов В.Г., Шепитько Г.Е. и др. – М.: ВНИИПО МВД СССР, 1983. – 110 с.

Статья поступила в редакцию Интернет-журнала 8 июля 2009 г.