Г.Е. Шепитько

АНАЛИТИЧЕСКИЕ ОЦЕНКИ ПОТЕНЦИАЛЬНОЙ БЕЗОПАСНОСТИ ОБЪЕКТА ПРИ ФИКСИРОВАННОМ РЕСУРСЕ ВНУТРЕННЕГО НАРУШИТЕЛЯ

Автором в данной работе впервые обосновано первое уравнение безопасности объекта. Приведены теоретические оценки предельной вероятности защиты объекта от внутреннего непреднамеренного нарушителя при неограниченных затратах на защитные мероприятия.

Ключевые слова: потенциальная безопасность, инцидент, модель Пуассона, уравнение безопасности, внутренний непреднамеренный нарушитель.

G.E. Shepitko

ANALYTICAL EVALUATION OF THE POTENTIAL SECURITY OF THE FACILITY WITH A FIXED RESOURCE OF INTERNAL VIOLATOR

The author of this paper for the first time proved the first equation of the security facility. He gives theoretical estimates of the probability of protecting the facility from the unintentional internal violator, with unbounded costs of protective measures.

Key words: potential security, incident, Poisson model, equation of security, unintentional internal violator.

Основная парадигма создаваемой теории безопасности объектов состоит в разрешении проблемы противостояния системы защиты объекта нарушителям и другим источникам угроз. Теоретическую и прагматическую значимость имеет при этом такой комплекс моделей безопасности, адекватность которых условиям практической деятельности подтверждается наличием не только объяснения существующих закономерностей, но и предсказанием новых результатов. В работах автора [1-5] рассмотрено несколько математических моделей безопасности, но специально не уделялось внимание оценке предельных возможностей существующих и прогнозируемых систем безопасности. В связи с этим назрела необходимость в опубликовании цикла теоретических работ по затронутой проблематике.

Целью работы является оценка потенциальных значений характеристик системы безопасности объекта при противостоянии непреднамеренному внутреннему нарушителю при условии, что известны и фиксированы ресурсы нарушителя.

Для корректности постановки задачи зафиксируем следующие исходные 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, связанные с противоправ-

ными действиями внутренних нарушителей. Ансамбль объектов защиты относится к множеству простых объектов категории важности КТ4 [6], на которые чаще всего посягаются заранее неподготовленные нарушители, неспособные совершенствовать свои приёмы нападения и совершать обход существующих средств защиты. Экономическая мощь системы защиты объекта и нарушителя характеризуется объёмами их ресурсов V и X соответственно в виде стоимости ежегодных затрат в валютных условных единицах. Инциденты безопасности являются редкими событиями, поэтому выполняется неравенство $K \le M\ N\ T$. Дополнительные физические ограничения в виде $M \le 1000, N \le 1000$, T= 1 год желательно учитывать для уменьшения затрат на проведение мониторинга состояния безопасности объектов и проверки адекватности математических моделей.

Теорема 1. При воздействии пуассоновского потока инцидентов внутренних непреднамеренных нарушителей с фиксированным ресурсом поведение автономной линейной системы защиты первого порядка с постоянными параметрами описывается первым уравнением безопасности вида

$$P(T) = \exp\{-\lambda_0\ T \exp[-(a + b\ (q - 1))\ T]\}, \quad (1)$$

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;

a, b – постоянные коэффициенты.

Доказательство.

Пусть задано количество инцидентов K(t) на поле [N, T] в момент времени $t = t_0 + T$. Допустим, что K (t + Δt) в последующий момент времени t + Δt прямо пропорционально значению K(t), плотности X ресурсов нарушителя и обратно пропорционально плотности V ресурсов системы защиты.

Тогда можно записать выражение для приращения количества инцидентов за интервал Δt :

$$[K(t + \Delta t) - K(t)]/\Delta t = b\ X\ K(t) - (a + b\ V)\ K(t). \quad (2)$$

Применяя оператор статистического усреднения к обеим частям уравнения (2) и разделяя их на значение N T, получим в пределе при $\Delta t \to 0$ дифференциальное уравнение первого порядка относительно интенсивности λ(t) инцидентов:

$$d\lambda(t) / dt = [b\ X - (a + b\ V)]\ \lambda(t). \quad (3)$$

Решение задачи Коши для этого уравнения имеет вид:

$$\lambda\ (T) = \lambda_0 \exp-[a + b\ (q - 1)\ X]\ T, \quad (4)$$

где

$$\lambda(T) = \langle K \rangle / N\ T; \quad (5)$$

<K> - статическое среднее количества инцидентов на N предметах защиты за период времени T;

λ(T) - интенсивность потока инцидентов на поле [N, T].

Если поток инцидентов на поле [N, T] является простейшим пуассоновским, тогда, ограничившись рассмотрением случайного процесса K(t) для всех предметов защиты N, можно записать выражение для распределения вероятностей одномерного закона Пуассона:

$$P(k, T)=[(\lambda T)^k / k!] \exp(-\lambda T), \quad (6)$$

где k - количество инцидентов на одном предмете защиты за период времени T.

Из рассмотрения (6) следует, что при К = 0 вероятность отсутствия инцидентов

$$P(T) = \exp(-\lambda T). \quad (7)$$

Тогда, с учётом выражения (4), получим искомое уравнение безопасности (1), что и требовалось доказать.

Следствие 1

Из формул (7) и (1) следует соотношение

$$P(T) = P_0(1 - P_{пр}), \quad (8)$$

где

$$P_0= \exp(-\lambda_0 T); \quad (9)$$

$$P_{прусл} = 1 - \exp(-\lambda_{усл} T). \quad (10)$$

Тогда вероятность пропуска инцидентов системой защиты определяется соотношением

$$P_{при} = P_0 P_{пр\ усл}, \quad (11)$$

где P_0 – потенциальная вероятность появления инцидентов (9);

$P_{пр\ усл}$ – условная вероятность пропуска инцидентов системой защиты (10).

Поэтому погрешность δ определения интенсивности инцидентов можно представить в виде логарифма коэффициента вариации в зависимости от количества инцидентов K:

$$\delta\ [\partial Б] = 20 \log 1/ K, \quad (12)$$

где

$$K = \lambda(q)\ T\ N\ M \quad (13)$$

На рис.1 представлены зависимости λ(q), $P_{усл}(q)$, δ(q), К(q), полученные при a = 0,3 , b = 0,5 , T = 1, N = 100, M = 1. Из рассмотрения этих зависимостей следует, что с погрешностью не более 3 *∂Б* можно оценить интенсивность редких инцидентов на одном объекте (λ = 0,005).

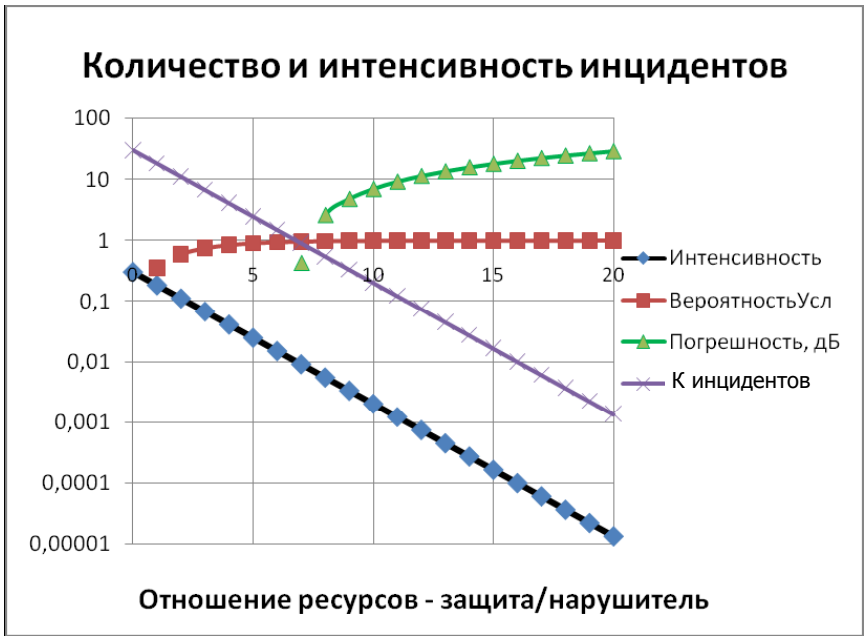

Рис. 1.

Таким образом, показано что, предельные значения интенсивности инцидентов непреднамеренного внутреннего нарушителя определятся только отношением ресурсов "система защиты – нарушитель", а надёжность оценки этой интенсивности зависит от объёма выборки T N M.

Литература

1. Шепитько Г.Е. Модель "Хищник-защита-ресурс" в управлении системой информационной безопасности / Труды XVI международной конференции "Проблемы управления безопасностью сложных систем PMECS". – М.: ИПУ РАН, 2008. - С. 197-199.

2. Шепитько Г.Е. Экономическая модель компьютерных нарушений/ Семнадцатая научно-техническая конференция "Системы безопасности" - СБ-2008. – М.: Академия ГПС МЧС России, 2008. – С. 60-63.

3. Шепитько Г.Е., Гудов Г.Н. Расчёт экономического риска системы защиты информации / Интернет-журнал "Технологии техносферной безопасности" - № 2. - 2006. - http://ipb.mos.ru/ttb.

4. Шепитько Г.Е. Проблемы охранной безопасности объектов / Под. ред. проф. В.А. Минаева. – М.: Русское слово, 1995. – 352 с.

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

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

Статья поступила в редакцию Интернет-журнала 26 мая 2009 г.