Расчет резерва времени для выполнения защитных мероприятий информационного объекта

Живов А. Д., Семенов А. Н., Гвоздева Г. А.
ФГБУ «4ЦНИИ» Минобороны России
Королев, Россия
4cnii@mil.ru

Аннотация. **На основе игровой модели информационной безопасности рассматривается система «нападение – защита». «Нападение» представлено последовательностью независимых случайных величин – интервалов времени выполнения целевых операций. Рассчитывается суммарная продолжительность этих интервалов – резерв времени для выполнения защитных мероприятий объекта. Начало отсчёта – обнаружение события разведывания объекта, конец – момент завершения возможной компьютерной атаки. Полученные результаты могут быть полезны при определении условий (требований) встраивания новых программно-аппаратных средств в общую систему обеспечения безопасности объектов.**

Ключевые слова: **нападение, защита, операция, интервал, разведывание, распределение, композиция, расчет.**

Введение

При построении систем защиты информации используются разнообразные методы и модели, среди них важное место занимают игровые модели. В частности, игровая модель системы защиты информации, которая используется для выбора решения, обеспечивающего оптимальное соотношение между затратами на средства защиты и снижением риска эксплуатации системы, рассматривается в [1].

В статье [2] изложены принципы количественного оценивания информационной безопасности с позиций теории игр. Введены определения игровой матрицы и ее количественной интерпретации. Представлены методики анализа, планирования и проектирования информационной безопасности на основе предложенных моделей.

В диссертационной работе [3] разработана игровая модель для обеспечения оптимальности системы защиты информации. Модель поиска оптимального проекта представляет собой игру статистика с природой, где под статистиком понимается владелец информационной системы, а под природой – злоумышленники.

В статье [4] рассматривается теоретико-игровая модель, с помощью которой решается задача оптимального выделения ресурсов кибер-безопасности, таких как время администратора для разных задач и др.

В работе [5] исследуются модели безопасности взаимодействий для различных вариантов игры, таких как слабое звено или лучший выстрел, чтобы представлять практические сценарии безопасности.

В [6] авторы решают проблему нахождения оптимального оборонительного покрытия. Из-за неопределенности действий атакующего они пытаются определить такое покрытие, максимизируя наихудший выигрыш над целями в наборе атаки. В игре для кибер-безопасности можно считать, что защитник не знает выигрыша для злоумышленника и может только оценить затраты.

В настоящей статье рассматривается система «нападение – защита», где сторона нападения представляет собой сложный пространственно распределенный комплекс средств, реализующий процесс разведывания, передачи, приема, обработки и интерпретации разведданных с возможным принятием и выполнением решения о компьютерной атаке объекта разведывания.

Для обеспечения безопасности последнего жизненно важно оперативно рассчитать вероятностно-временные характеристики случайной величины – продолжительности этого процесса (т. е. искомого резерва времени). В данной статье приведена схема расчета суммарной плотности распределения упомянутой величины и соответственной функции распределения. Полученные результаты содержат полную информацию для принятия решения о выполнении защитных мероприятий.

Модель «нападения»

Модель «нападения» представлена последовательностью независимых случайных величин $t_1, t_2, t_3, \ldots, t_i, \ldots, t_n$ – значений интервалов времени выполнения целевых операций компонентами указанного комплекса.

К значениям t_i интервалов времени «прикреплены» соответственные распределения плотности вероятностей $\varphi(t_i)$ (рис. 1). Распределение $\varphi(T_\Sigma)$ описывает плотность распределения суммы T_Σ – искомого резерва времени (также случайной величины). Интеграл распределения $\varphi(T_\Sigma)$ является функцией распределения $F(T_\Sigma)$.

В зависимости от меняющихся условий обстановки сторона «нападения» меняет состав и конфигурацию компонентов разведывательно-атакующего комплекса, порождая тем самым различные (ситуационные) последовательности, отличающиеся составом интервалов t_i, их распределениями $\varphi(t_i)$ и в конечном счёте – распределениями $\varphi(T_\Sigma)$ и $F(T_\Sigma)$.

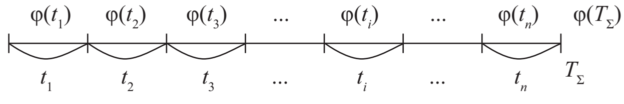

Рис. 1. Схема описания плотности $\varphi(T_\Sigma)$

Модель «защиты»

Сторона «защиты» обладает:

• достаточно достоверным знанием структуры существующих комплексов стороны «нападения»;

• свойством в реальном времени обнаруживать события разведывания объекта информатизации;

• приблизительным знанием временны́х характеристик операций, выполняемых потенциальным нарушителем;

• возможностью выполнять защитные мероприятия за допустимое время T^*, располагая резервом времени T_Σ.

Постановка задачи

Ставится задача: рассчитать распределения $\varphi(T_\Sigma)$ и $F(T_\Sigma)$ для обоснования решения по выполнению защитных мероприятий согласно критерию

$$F(T_\Sigma) = P\left[T_\Sigma >> T^*\right], \tag{1}$$

где $P\left[T_\Sigma >> T^*\right]$ – вероятность того, что объект разведывания (возможная цель) располагает достаточным резервом времени для выполнения защитных мероприятий. Символ >> означает, что «лицо, принимающее решение», неформально оценивая риск возможной атаки, назначает для суммы T_Σ некоторый «запас», значение которого зависит от степени доверия к результатам расчёта рассматриваемых распределений.

Решение задачи

Применительно к заданной ситуационной последовательности схема решения задачи представляется следующим образом.

Распределение суммы независимых случайных величин $\varphi(T_\Sigma)$, будучи композицией распределений $\varphi(t_i)$, рассчитывается по правилам вычисления их свёрток. Сначала вычисляется распределение $\varphi(t_{1,2})$ суммы первых двух независимых случайных величин (значений t_1 и t_2) путём расчёта свёртки согласно формуле [7, 8]

$$\varphi(t_{1,2}) = \varphi(t_1)\cdot\varphi(t_2) = \int\limits_0^\infty \varphi(t_1)\varphi(t_2 - t_1)dt, \tag{2}$$

где * – символ свертки.

Далее рассчитывается последовательность свёрток:

$$\begin{gathered}\varphi(t_{1,2})\cdot\varphi(t_3) = \varphi(t_{1,2,3});\\ \varphi(t_{1,2,3})\cdot\varphi(t_4) = \varphi(t_{1,2,3,4});\\ \varphi(t_{1,2,3,\dots,}t_{n-1})\cdot\varphi(t_n) = \varphi(T_\Sigma).\end{gathered} \tag{3}$$

Функция распределения $F(T_\Sigma)$ рассчитывается интегрированием полученного распределения $\varphi(T_\Sigma)$. Результаты расчёта, описывающие распределения $\varphi(T_\Sigma)$ и $F(T_\Sigma)$, представляются в символьном (формула) и в графическом виде. Задача решена.

Аналогичным образом рассчитываются другие ситуационные последовательности.

Полученные результаты содержат полную информацию, необходимую для анализа и принятия решения согласно критерию (1).

Достоверность результатов расчёта зависит от точности приведения модели «нападения» в соответствие с составом и вероятностно-временными характеристиками компонентов действующего разведывательно-атакующего комплекса (задача структурной и параметрической идентификации).

В идеале «защита» должна располагать структурой (формулой) и параметрами каждого распределения $\varphi(t_i)$.

Однако получить от действующих компонентов рассматриваемого комплекса опытные данные относительно продолжительности выполнения каждой операции и в достаточном объёме проблематично. Это обстоятельство актуализирует задачу добывания необходимых сведений из всех доступных источников.

На практике обычно исходят из допущения, что случайные величины t_i распределены по экспоненциальному закону:

$$\varphi(t_i) = \lambda_i \exp(e^{-\lambda_i t_i}), \tag{4}$$

где $\lambda_i = 1/\tau_i$ – параметр экспоненциального распределения; τ_i – среднестатистическое значение времени выполнения i-й операции.

В этом случае распределения $\varphi(T_\Sigma)$ и $F(T_\Sigma)$ описываются обобщённым законом Эрланга n-го порядка [7], согласно которому математическое ожидание (МО) и дисперсия (Д) указанных распределений рассчитываются по простым формулам:

$$MO = \sum_1^n 1\Big/\lambda_i = \sum_1^n \tau_i;\ Д = \sum_1^n 1\Big/\lambda_i^2 = \sum_1^n \tau_i^2. \tag{5}$$

Экспоненциальное распределение случайной величины t_i предполагает, что в большинстве случаев i-я операция выполняется относительно быстро, что не всегда соответствует практике. Рассмотрим возможность применения другого вида распределения.

В нашем случае наибольший вклад в сумму T_Σ вносят операции, продолжительность которых варьируется в известных пределах от минимального (t_{min}) до максимального (t_{max}) значения и может быть очень велика. На практике значения этих пределов с приемлемой точностью известны по данным от отечественных аналогов.

Для формального описания подобного вида распределений мировое сообщество испытателей разработало двухпараметрическое семейство бета-распределений [9]. Каждый экземпляр такого семейства представлен аналитическим выражением, значения параметров которого определяют форму графика и подобраны сообразно физической сущности рассматриваемого процесса.

Плотность бета-распределения описывается формулой

$$\varphi(t) = \frac{1}{B(\alpha,\beta)} t^{\alpha-1}(1-t)^{\beta-1}, \tag{6}$$

где $B(\alpha,\beta)$ – бета-функция. В семействе бета-распределений в нашем случае наиболее приемлем экземпляр с параметрами формы $\alpha = 2$ и $\beta = 5$ (рис. 2).

Бета-функция рассчитывается через Гамма-функции:

$$B(\alpha,\beta) = B(2,5) = B(\alpha)B(\beta)\big/B(\alpha+\beta) = B(2)\cdot B(5)\big/B(7).$$

Математическое ожидание и дисперсия бета-функции равны, соответственно, $\alpha/\alpha + \beta$ и $\alpha\beta\big/(\alpha+\beta)^2(\alpha+\beta+1)$.

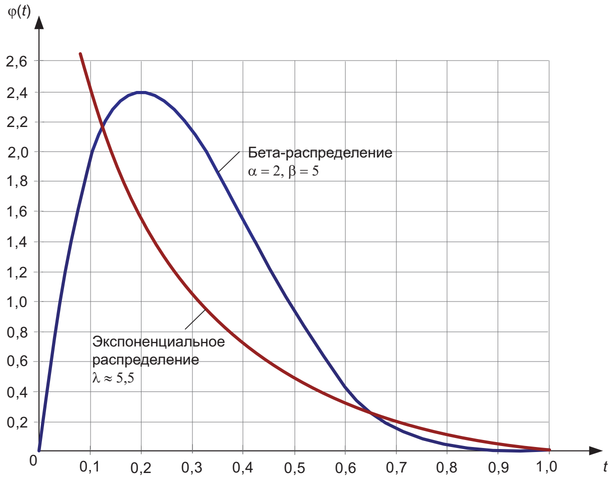

Рис. 2. Плотность экспоненциального и бета-распределений

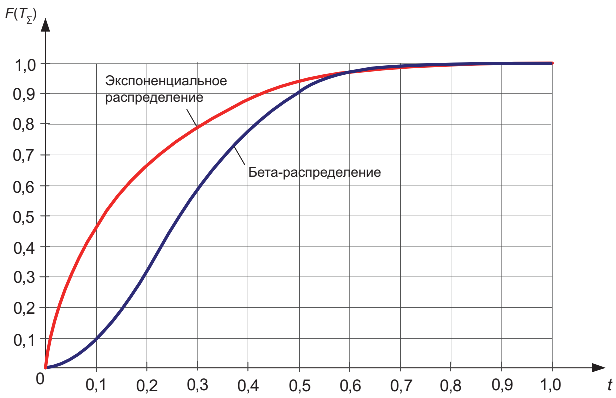

Рис. 3. Функции экспоненциального и бета-распределений

На рис. 3 совмещены два графика плотности вероятности случайной величины t_i: для стандартного бета-распределения, сосредоточенного на условной временно́й базе – отрезке от нуля до единицы, и экспоненциального распределения, параметр которого ($\lambda \approx 5{,}5$) подобран так, чтобы график этого распределения уместился на общей временно́й базе.

Гамма-функции рассчитываются по правилу [10]: $B(n) = (1-n)!$. Для значений $n = 2, 5, 7$ имеем: $B(2) = 1$; $B(5) = 24$; $B(7) = 720$.

Отсюда $B(\alpha, \beta) = B(2, 5) = 24/720 = 1/30$, а выражение (6) приобретает вид $\varphi(t) = 0{,}33t(1-t)^4$.

На рис. 3 приведены два графика соответственных функций распределения.

Формулы и значения числовых характеристик для вышеприведённых распределений сведены в таблицу.

При практических расчётах отрезку от нуля до единицы (условной временно́й базе) следует придавать смысл от t_{min} до t_{max} временных единиц (минут, часов и др.).

Сравнительные характеристики экспоненциального и бета-распределений

Распределение	Математическое ожидание	Дисперсия
Бета-распределение	$\alpha/\alpha+\beta \approx 0{,}28$	$\alpha\beta/(\alpha+\beta)^2\,(\alpha+\beta+1) \approx 0{,}025$
Экспоненциальное	$1/\lambda \approx 0{,}18$	$1/\lambda^2 \approx 0{,}033$

Нетрудно оценить, насколько велико различие суммарных значений T_Σ для рассмотренных распределений. Целесообразность описания бета-распределением случайных величин t_i, для которых с приемлемой точностью известны значения их границ, подтверждается, если измеренные опытным путём значения t_i) будут группироваться вблизи теоретического значения математического ожидания, равного 0,28 ($t_{max} - t_{min}$).

Заключение

Естественным продолжением данной статьи должна стать серия модельных экспериментов, реализующих расчёты согласно последовательности (3) при различных комбинациях исходных данных.

Результаты расчёта необходимо проанализировать и тематически обработать, чтобы:

• определить основные закономерности изменения формы графиков распределений $\varphi\ (T_\Sigma)$ и $F\ (T_\Sigma)$;

• подтвердить или отвергнуть утверждение о применимости обобщённого закона Эрланга n-го порядка к любым распределениям;

• определить правила практического применения «защитой» результатов расчёта.

Приведенные в статье результаты могут быть полезны при определении условий (требований) встраивания новых программно-аппаратных средств в общую систему обеспечения безопасности информационных объектов.

Литература

1. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М. : МИФИ, 1997. – 537 с.

2. Шахов В. Г. Игровые и топологические модели информационной безопасности / В. Г. Шахов, А. В. Морозов, А. П. Тиунов, А. Н. Громов // Изв. Транссиба. – 2015. – № 1 (21). – С. 89–94.

3. Арьков П. А. Разработка комплекса моделей для выбора оптимальной системы защиты информации в информационной системе организации : дис. … канд. техн. наук. – Волгоград, 2009. – 185 с.

4. Fielder A. Game Theory Meets Information Security Management / A. Fielder, E. Panaousis, P. Malacaria, C. Hankin1, F. Smeraldi; eds. N. Cuppens-Boulahia et al. // IFIP Int. Federation for Information Proc. SEC 2014. – IFIP AICT 428 б 2014. – P. 15–29.

5. Grossklags J. Secure or insure? A game-theoretic analysis of information security games / J. Grossklags, N. Christin, J. Chuang // Proc. of the 17th Int. Conf. on World Wide Web «WWW 2008». – ACM, 2008. – P. 209–218.

6. Kiekintveld C. Security games with interval uncertainty / C. Kiekintveld, T. Islam, V. Kreinovich // Proc. 12th Int. Conf. on Autonomous Agents and Multiagent Systems «AAMAS 2013». – Int. Foundation for Autonomous Agents and Multiagent Systems, Richland, 2013. – P. 231–238.

7. Вентцель Е. С. Теория вероятностей и её инженерные приложения / Е. С. Вентцель, Л. А. Овчаров. – М. : Наука, 1988. – 480 с.

8. Шор Я. Б. Статистические методы анализа и контроля качества и надёжности / Я. Б. Шор. – М. : Сов. Радио, 1962. – 552 с.

9. Бета-распределение. http://ru.wikipedia.org

10. Бронштейн И. Н. Справочник по математике / И. Н. Бронштейн, К. А. Семендяев. – М. : Наука, 1962. – 608 с.

The Calculation of Time Reserve for the Execution of Protective Actions of Information Object

Zhivov, A. D., Semenov A. N., Gvozdeva G. A.
FSBI "4 CRI defense of Russia"
Korolyov, Russia
4cnii@mil.ru

Abstract. **Based on the game model of information security system is considered "attack-defense". «Attack» is a sequence of independent random variables – time intervals for performing target operations. The total length of these time intervals – time reserving for the implementation of protective actions of an object – is calculated. The beginning of the countdown – the event consisting in the fact that the object is detected, the end of the countdown – the moment of completion of a possible computer attack. The obtained results can be useful in determining the conditions (requirements) of embedding new software and hardware into the overall system of safety of objects.**

Keywords: **attack, defense, interval, detection, distribution, composition, calculation.**

References

1. Gerasimenko V.A., Maluk A.A. *Osnovy zashchity informatsii* [Information Protection Basics], Moscow, MIFI, 1977, 537 p.

2. Shakhov V. G., Morosov A. P., Tiunov A. N. Gambling and topological information security model [Igrovye i topologicheskie modeli informatsionnoi bezopasnosti], *Izvestiia Transsiba [Proc. Trans-Sib]*, 2015, no. 1 (21), pp. 89-94.

3. Arkov P.A. *Razrabotka kompleksa modelei dlya vybora optimal'noi sistemy zashchity informatsii v informatsionnoy sisteme organizatsii* [Development of complex models to select optimal system of information protection in information systems of the organization. Diss. on competition of a sci. degree Cand. tech. Sci.], Volgograd, 2009, 185 p.

4. Fielder A., Panaousis E., Malacaria P., Hankin C., Smeraldi F. Game Theory Meets Information Security Man-agement; eds. N. Cuppens-Boulahia et al. *IFIP Int. Federation for Information Proc.*, SEC 2014, IFIP AICT 428, pp. 15-29.

5. Grossklags J., Christin N., Chuang J. Secure or insure? A game-theoretic analysis of information security games, *Proc. 17th Int. Conf. on World Wide Web "WWW 2008"*, ACM, 2008, pp. 209-218.

6. Kiekintveld C., Islam T., Kreinovich V. Security games with interval uncertainty, *Proc. 12th Int. Conf. on Autonomous Agents and Multiagent Systems "AAMAS 2013"*, Int. Foundation for Autonomous Agents and Multiagent Systems, Richland, 2013, pp. 231-238.

7. Venttsel' E.S., Ovcharov L.A. *Teoriya veroiatnostey i eyo inzhenernye prilozheniya*. [Probability theory and its engineering applications], Moscow, Nauka, 1988, 480 p.

8. Shor Ia.B. Statisticheskie metody analiza i kontrolia kachestva i nadezhnosti [Statistical methods of analysis and control of quality and reliability], Moscow, Sovietskoye radio, 1962, 552 p.

9. http://ru.wikipedia.org > Beta-distribution.

10. Bronshtein I. N., Semendyaev K. A. *Spravochnik po matematike* [Handbook of mathematics], Moscow, Nauka, 1962, 608 p.