УДК 004.056

А.С. Кабанов, А.Б. Лось, В.И. Трунцев

Временная модель оценки риска нарушения информационной безопасности

Излагаются результаты по построению оценок риска нарушения информационной безопасности с учетом времени работы вычислительной системы. Рассмотрены математические модели построения DoS-атак на сервер информационной системы.

Ключевые слова: временная модель, оценка риска, время эксплуатации.

Анализ отечественных и международных стандартов по информационной безопасности [1, 2] показывает, что в настоящее время решение вопросов оценки качества защиты информационных систем, мягко говоря, оставляет желать лучшего. Основное требование стандартов – оценка рисков при нарушениях информационной безопасности (ИБ). При этом отсутствует единый подход к решению данной задачи и четкие методические указания по реализации процедур построения указанных оценок. В результате в лучшем случае каждый эксперт разрабатывает свой подход к решению поставленной задачи, а в большинстве случаев задача оценки рисков, по существу, сводится к проведению стендовых испытаний разработанной системы информационной безопасности (ИБ).

Кроме того, по нашему мнению, сами по себе оценки рисков нарушения ИБ не могут характеризовать уровень обеспечения безопасности, а главное – не дают представления о возможности или невозможности эксплуатации данной информационной системы (ИС). Представляется целесообразным строить оценки рисков ИБ на основе хотя бы простейших стандартных прогнозных моделей, учитывающих их изменение с течением времени. Такой подход позволит ввести единую и понятную даже неспециалисту характеристику ИС с точки зрения обеспечения ИБ – *время безопасной работы информационной системы*. В этом случае заказчики ИС будут иметь четкое представление о возможности или невозможности ее эксплуатации в течение определенного промежутка времени. Ниже приводятся некоторые соображения по поводу построения указанных прогнозных моделей.

В традиционном подходе к проблеме оценки риска нарушения информационной безопасности (ИБ), который можно назвать статическим, величина риска R находится из соотношения

$$R=\sum_{i=1}^{n} p(y_i)\cdot u_i,$$

где $p(y_i)$ – вероятность реализации злоумышленником угрозы нарушения ИБ y_i; u_i – величина ущерба от успешного осуществления данной угрозы, $i=1,2,...,n$.

В рамках этой модели нарушителя предполагается, что он начинает действовать с момента начала работы ИС и атакует ее с неизменной интенсивностью. Такой подход, во-первых, в ряде случаев приводит к неоправданному завышению рисков ИБ, что в свою очередь влечет излишнюю усложненность подсистемы ИБ в общей ИС, а также затруднения в ходе эксплуатации последней, а во-вторых, как было указано выше, не дает представления о сроках безопасной эксплуатации ИС.

Очевидно, что в общем случае вероятность успешной реализации данной угрозы $p(y_i)$ и величина ущерба от ее реализации u_i зависят от времени, прошедшего с начала эксплуатации системы:

$$p(y_i)=p_{y_i}(t),\quad u_i=u_i(t).$$

Зависимость величины риска R от момента времени t при этом имеет вид

$$R(t)=\sum_{i=1}^{n} p_{y_i}(t)\cdot u_i(t).$$

Функции $p_{y_i}(t)$ и $u_i(t)$ являются, как правило, неубывающими функциями времени t, и, следовательно, величина риска $R(t)$ также возрастает с ростом t.

Вводя границу величины безопасного риска R_0, можно вычислить значения параметра T_o – *времени безопасной эксплуатации ИС*, являющегося решением уравнения

$$R(x)=\sum_{i=1}^{n} p_{y_i}(x)\cdot u_i(x)=R_0. \quad (1)$$

В качестве функций $p_{y_i}(t)$ и $u_i(t)$ могут быть выбраны, например, функции, наиболее часто встречающиеся в моделях такого типа:

$$p_{y_i}(t)=p_i^{(0)}\cdot(1-e^{-\alpha_i\cdot t}),\ u_i(t)=u_i^{(0)}\cdot(1-e^{-\beta_i\cdot t}), \quad (2)$$

где $p_i^{(0)}$ и $u_i^{(0)}$ – величины, соответствующие статическим значениям вероятности успешной реализации угрозы y_i и величины ущерба от ее успешной реализации; α_i и β_i – соответствующие параметры прогнозной модели.

Для вычисления параметров $p_i^{(0)}$, $u_i^{(0)}$, α_i, ..., β_i данной прогнозной модели могут применяться как статистические методы, учитывающие опыт эксплуатации рассматриваемой ИС, так и другие известные методы, в частности, метод экспертных оценок.

Для рассматриваемых прогнозных функций $p_{y_i}(t)$ и $u_i(t)$ величина риска имеет вид

$$R(t)=\sum_{i=1}^{n} p_i^{(0)}\cdot(1-e^{-\alpha_i\cdot t})\cdot u_i^{(0)}\cdot(1-e^{-\beta_i\cdot t}).$$

Заметим, что прогнозные модели, представленные в выражении (2), уже применялись в своих исследованиях рядом авторов [3].

В качестве примера применения предлагаемого подхода рассмотрим распределенную платежную систему (РПС) на основе банковских карт (БК) с магнитной полосой и модель несанкционированного доступа типа «кража информации во время ее хранения». В этом случае атака нарушителя и ее блокирование состоят из нескольких этапов: выбор хранилища для анализа (время реализации t_1), обнаружение в выбранном хранилище области авторизационных запросов (время реализации t_2), взлом области авторизационных запросов, похищение информации с действующих БК (время реализации t_3), блокирование доступа (время реализации t_4). В этом случае простейшая модель вероятности успешной реализации данной атаки имеет вид

$$p_y(t)=(1-e^{-\alpha\cdot t}),$$

где $\alpha=\dfrac{1}{t_1+t_2+t_3+t_4}$.

Нетрудно видеть, что вероятность успешной реализации данной атаки уменьшается с увеличением общего времени действия нарушителя, включая время срабатывания блокировки.

Пусть значение возможного ущерба u от успешной реализации рассматриваемой атаки является постоянной величиной и не зависит от времени. Тогда уравнение для определения параметра τ_0 – *времени безопасной работы информационной системы – имеет вид*

$$u\cdot(1-e^{-\alpha\cdot t})=R_0,$$

а решением данного уравнения является величина

$$T_0=\frac{1}{\alpha}\cdot\ln\frac{u}{u-R_0}. \quad (3)$$

Аналогично могут быть построены и другие модели попыток несанкционированного доступа нарушителя, например модель, предполагающая изменение информации на магнитной карте.

Рассмотрим еще один пример применения данного подхода на основе прогнозирования успешных реализаций DoS-атак на информационные системы. Пусть в информационной системе имеется один сервер, на который злоумышленник пытается реализовать DoS-атаку типа «отказ в обслуживании» путем генерации потока запросов с разных адресов. Предполагается, что максимальное число запросов, обрабатываемых сервером в единицу времени, равно m_0. При превышении данного числа запросов в единицу времени сервер блокируется, перестает обслуживать запросы и атака считается успешно реализованной.

Для проведения численных расчетов будем предполагать, что вероятностное распределение числа запросов, поступающих на сервер в единицу времени, является стационарным и подчиняется

закону Пуассона с параметром λ. Вероятностные модели такого типа часто применяются в системах массового обслуживания [4]. При этом вероятность $p(m)$ поступления на сервер ровно m запросов в единицу времени имеет вид

$$p(m)=\frac{e^{-\lambda}\cdot\lambda^{m}}{m!}.$$

Из сделанных выше предположений следует, что штатный режим работы сервера обеспечивается в случае, когда число заявок, поступающих на него в единицу времени, не превышает величины m_0, вероятность данного события $p_{\text{шт}}$, очевидно, имеет вид

$$p_{\text{шт}}=\sum_{k=0}^{m_0}\frac{e^{-\lambda}\cdot\lambda^{k}}{k!}.$$

Обозначим через Ω_t событие, состоящее в успешной реализации DoS-атаки в течение t единиц времени. Нетрудно видеть, что вероятность этого события равна

$$p(\Omega_t)=1-p^{t}_{\text{шт}}=1-(1-q)^{t},$$

где $q=1-p_{\text{шт}}$.

При достаточно малых значениях вероятности q имеет место соотношение $(1-q)^{\frac{1}{q}}\approx e^{-1}$, поэтому для вероятности $p(\Omega_t)$ справедливо равенство

$$p(\Omega_t)\approx 1-e^{-q\cdot t}.$$

Пусть, как и в предыдущем примере, значение возможного ущерба u от успешной реализации рассматриваемой атаки является постоянной величиной и не зависит от времени и среднее значение допустимого ущерба равно R_0. Тогда, учитывая соотношение (3), для времени безопасной эксплуатации информационной системы T_0 получаем

$$T_0=\frac{1}{q}\cdot\ln\frac{u}{u-R_0}. \qquad (4)$$

Рассмотрим случай, когда блокировка сервера происходит при поступлении более m_0 запросов в течение промежутка времени τ. В этом случае вероятность работы системы в штатном режиме в течение промежутка времени τ имеет вид

$$p_{\text{шт}}(\tau)=\sum_{k=0}^{m_0}\frac{e^{-\lambda\tau}\cdot(\lambda\tau)^{k}}{k!}.$$

Вероятность $p(\Omega_t)$ успешной реализации DoS-атаки в течение времени t может быть оценена величиной

$$p(\Omega_t)=1-(p_{\text{шт}}(\tau))^{\frac{t}{\tau}}=1-(1-q(\tau))^{\frac{t}{\tau}}\approx 1-\exp\{-q(\tau)\cdot t/\tau\},$$

где $q(\tau)=1-p_{\text{шт}}(\tau)$.

Аналогично (4) для времени безопасной эксплуатации информационной системы T_0 получаем

$$T_0=\frac{\tau}{q(\tau)}\cdot\ln\frac{u}{u-R_0}.$$

Рассмотрим более строгую постановку задачи осуществления DoS-атаки. Пусть в дискретные моменты времени (t = 1, 2, …) реализуются случайные события в виде поступления или непоступления заявки на сервер. Пусть δ_i – индикатор события, состоящего в поступлении заявки на сервер в момент времени i. Будем предполагать, что δ_i – независимые, одинаково распределенные случайные величины и $p\{\delta_i=1\}=p$. Задача вычисления вероятности успешной реализации DoS-атаки в течение T моментов времени при условии, что блокировка сервера происходит в случае поступления более m_0 запросов в течение промежутка времени τ, состоит в следующем.

Определим случайные величины

$$\zeta_k = \delta_k + \delta_{k+1} + ... + \delta_{k+\tau-1},\ k = 1,2,...,$$

– количество событий (поступивших запросов) в течение времени τ, начиная с момента времени k, $k = 1,2,...$.

Во введенных обозначениях вероятность $p(\Omega_T)$ проведения успешной DoS-атаки за время T имеет вид

$$p(\Omega_T) = p\{\max_{1 \le k \le T-\tau+1} \zeta_k > m_0\}. \quad (5)$$

Последовательность $\{\zeta_k\}_{k=1}^{\infty}$, образованная из независимых случайных величин $\{\delta_k\}_{k=1}^{\infty}$, в научной литературе называется процессом скользящего суммирования или частичными суммами Эрдеша–Реньи, а изучению их характеристик посвящено довольно много работ. В работах [5] и [6] найдена асимптотика умеренных уклонений статистики $\max_{1 \le k \le T-\tau+1} \zeta_k$. В [7] получено явное выражение для константы в асимптотике вероятностей больших уклонений с условием Крамера. В форме условных предельных теорем описаны траектории блуждания, на которых осуществляется большое уклонение. В работе [8] найдено предельное значение функции распределения статистики $\max_{1 \le k \le T-\tau+1} \zeta_k$ при $T, \tau \to \infty$ и $T/\tau \to \varepsilon = \text{const}$.

Вычислив значение вероятности (5) и применяя соотношение (4), нетрудно получить время T_0 безопасной работы информационной системы.

Рассмотрим поставленную выше задачу исследования эффективности DoS-атак в терминах теории массового обслуживания. В этом случае задача вычисления вероятности $p(\Omega_T)$ успешной реализации DoS-атаки в течение времени T состоит в следующем.

Определим простейший поток событий – поступления заявок на сервер, в котором промежутки времени $X_1, X_2, ..., X_N, ...$ между последовательными событиями являются независимыми, одинаково распределенными случайными величинами с функцией распределения $p\{X_i < t\} = 1 - e^{-\lambda \cdot t}$, где λ – плотность потока событий (среднее число событий, приходящееся на единицу времени).

Определим случайные величины

$$\xi_k = X_k + X_{k+1} + ... + X_{k+m_0},\ k = 1,2,...,$$

– время поступления серии из $m_0 + 1$ событий, начиная с события с номером k, $k = 1,2,...$.

Обозначим через η_T – случайную величину, равную общему числу событий за время T.

Во введенных обозначениях вероятность $p(\Omega_T)$ проведения успешной DoS-атаки за время T имеет вид

$$p(\Omega_T) = \sum_{s=0}^{m_0} p\{\eta_T = n\} \cdot p\{\Omega_T / \eta_T = n\}, \quad (6)$$

где $p\{\eta_T = n\} = \dfrac{(\lambda T)^n \cdot e^{-\lambda T}}{n!}$,

$$p\{\Omega_T / \eta_T = n\} = p\{\max_{1 \le k \le n-m_0} \xi_k \le \tau\}.$$

Для вычисления вероятности $p\{\max_{1 \le k \le n-m_0} \xi_k \le \tau\}$ справедливы замечания, высказанные выше для вычисления вероятности $p\{\max_{1 \le k \le T-\tau} \zeta_k > m_0\}$.

Вычислив значение вероятности (6) и применяя соотношение (4), нетрудно получить время T_0 безопасной работы информационной системы.

В общем случае, например в случае зависимости возможного ущерба от времени или в случае появления нескольких потенциальных угроз, для решения уравнения (1) могут применяться и другие, в частности численные, методы.

Представляется, что предложенный выше подход к исследованию уровня защищенности ИС, основанный на оценке параметра T_0 – *времени ее безопасной работы*, может служить удобным инструментом, характеризующим качество защиты ИС.

Литература

1.Международный стандарт информационной безопасности ISO/IEC 17799–2005. Информационная технология -Методы защиты – Практическое руководство для менеджмента информационной безопасности [Электронный ресурс]. – Режим доступа: http://www.klubok.net/Downloads-index-redviewdownloaddatails-lid-362.html, свободный (дата обращения: 22.05.2010).

2. Российский стандарт информационной безопасности Р ИСО\МЭК 17799–2005. Информационная технология. Практические правила управления информационной безопасностью [Электронный ресурс]. – Режим доступа: http://gostexpert.ru/gost/gost-17799-2005, свободный (дата обращения: 22.05.2010).

3. Менжулин Р.В. Распределенные платежные системы на основе банковских карт с магнитной полосой: моделирование и регулирование рисков несанкционированного доступа к информации: автореф. дисс… канд. техн. наук. – Воронеж, 2011. – 21 с.

4. Венцель Е.С. Теория вероятностей: учеб. для вузов / Е.С. Венцель. – М.: Высшая школа. – 1999. – 575 с.

5. Питербарг В.И. О больших скачках случайного блуждания // Теория вероятностей и ее применения. – 1997. – Т. 36, вып. 1. – С. 54–64.

6. Довгалюк В.В. Большие уклонения траекторий пуассоновского процесса/ В.В. Довгалюк, В.И. Питербарг. – Вероятностные процессы и их приложения. – М.: МИЭМ. – 1989.– С. 112–117.

7. Козлов М.В. О частичных суммах Эрдеша–Реньи: Большие уклонения, условное поведение // Теория вероятностей и ее применения. – 2001. – Т. 46, вып. 4. – С. 678–696.

8. Лось А.Б. О предельном распределении максимума процесса скользящего суммирования (частичных сумм Эрдеша–Реньи) // Вестник Московского государственного университета леса. – 2011. – №3(79). С. 185–189.

Кабанов Артем Сергеевич
Канд. техн. наук, доцент каф. «Информационная безопасность» Московского института электроники и математики (МИЭМ)
Национального исследовательского университета «Высшая школа экономики» (НИУВШЭ)
Тел.: 8-903-557-73-97
Эл. почта: kabanov_as@mail.ru

Лось Алексей Борисович
Канд. техн. наук, доцент, зав. каф. «Информационная безопасность» МИЭМ НИУВШЭ
Тел.: 8-910-477-88-27
Эл. почта: alexloss@miem.edu.ru

Трунцев Вадим Игоревич
Ст. преподаватель каф. «Информационная безопасность» МИЭМ НИУВШЭ
Тел.: 8-905-525-00-11
Эл. почта: bugtract@rambler.ru

Kabanov A.S., Los A.B., Truntsev V.I.

Temporary model assessment of the risk of information security

The article presents the results of the construction risk assessments of information security for time-sensitive information system. Considered mathematical models of the DoS attak on the server of the information system.
Keywords: Temporary model, assessment of the risk, time-sensitive.