

АНАЛИЗ МОМЕНТА ВРЕМЕНИ СОВЕРШЕНИЯ БЛИЖАЙШЕЙ ЗЛОУМЫШЛЕННОЙ АТАКИ В СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ АППАРАТА РЕДКИХ РЕГЕНЕРИРУЮЩИХ ПРОЦЕССОВ

Г. А. Попов, Е. А. Попова

*Астраханский государственный технический университет,
Астрахань, Российская Федерация*

Проводится анализ модели, описывающей процесс атак на защищаемый объект, где хранится закрытая информация, построенной на основе аппарата регенерирующих последовательностей успешного завершения злонамеренных атак. Именно, моменты реализации атак рассматриваются как точки регенерации атак, т. е. предполагается, что различные атаки независимы. Предполагается, что атаки, исходящие из одного источника, происходят достаточно редко, носят изолированный единичный характер и достаточно далеко разнесены во времени, т. е. событие успешного совершения атаки является редким событием, но потери при ее успешном завершении могут быть огромными. В качестве исследуемой характеристики выбран ближайший момент, когда очередная атака окажется успешной, – эта характеристика является одной из наиболее важных с точки зрения информационной безопасности. Знание параметров данной характеристики позволит на соответствующих временных интервалах предпринимать дополнительные действия, повышающие уровень обеспечения защиты. Исследования проводятся при предположении неоднородности всех характеристик модели, что более адекватно соответствует реальному состоянию в системах информационной безопасности. Получено асимптотическое соотношение для момента совершения ближайшей успешной злонамеренной атаки в условиях, когда интервал времени, на котором проводится анализ атак, неограниченно растет, и одновременно вероятности совершения атак становятся все более редкими, причем эти величины изменяются согласованным образом.

Ключевые слова: информационная безопасность, объект защиты, момент ближайшей успешной атаки, регенерирующие процессы, редкие события.

Для цитирования: Попов Г. А., Попова Е. А. Анализ момента времени совершения ближайшей злоумышленной атаки в системе информационной безопасности на основе аппарата редких регенерирующих процессов // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2020. № 2. С. 34–44. DOI: 10.24143/2072-9502-2020-2-34-44.

Введение

Одна из типовых моделей, описывающих процесс атак на защищаемый объект, где хранится закрытая информация, может быть описана посредством аппарата регенерирующих последовательностей успешного завершения атак. Именно, моменты реализации атак рассматриваются как точки регенерации атак, т. е. предполагается, что различные атаки независимы. Доводом в пользу справедливости данного предположения является следующая особенность атак: в системах с хорошо организованной системой обеспечения информационной безопасности (ИБ) атаки обычно происходят достаточно редко, носят изолированный единичный характер и достаточно далеко разнесены во времени. То есть соответствующий регенерирующий процесс совершения атак имеет очень малую интенсивность. Более того, вероятность успешного завершения атаки также очень мала, что позволяет говорить о факте успешного совершения атаки как о редком событии. Несмотря на малую вероятность успешного завершения атак и редкость самих атак, процесс совершения атак на объект защиты необходимо анализировать, поскольку очень часто в случае успешности атаки потери, которые понесет объект защиты, могут оказаться огромными. Это справедливо как для злоумышленных атак, так и для незлоумышленных, в частности для стихийных событий природного характера, техногенных аварий.

Таким образом, процесс совершения атак на объект защиты достаточно адекватно описывается восстанавливаемыми системами с исчезающе малой вероятностью проявления некоторого события (успешной атаки) в моменты регенерации (восстановления) процесса [1–3]. С точки

зрения обеспечения ИБ наиболее важной характеристикой является ближайший момент, когда очередная атака окажется успешной. В терминологии регенерирующих процессов речь идет о моменте первого наступления некоторого (редкого) события [2]. Данная характеристика является случайной, поскольку все характеристики описанного регенерирующего процесса, вообще говоря, случайны. Тем не менее, можно оценить наиболее вероятные интервалы успешного завершения атак и предпринимать на этих интервалах дополнительные действия, повышающие уровень обеспечения защиты, например профилактические и проверочные мероприятия.

Для анализа момента возникновения редких событий в регенерирующих процессах очень часто используется известная теорема А. Д. Соловьева [4] для однородных регенерирующих процессов. Однако в системах ИБ условие однородности не выполняется по целому ряду причин, в частности, постоянно меняются характеристики атак. Это относится как к природным явлениям и техногенным событиям, так и к злонамеренным атакам, т. к. злоумышленники активны в поиске новых путей и возможностей проникновения на объект защиты. Кроме того, устаревает имеющееся программно-аппаратное и техническое обеспечение систем обеспечения ИБ. Поэтому при анализе вероятности совершения злонамеренной атаки необходимо учитывать изменяющийся нефиксированный уровень этой характеристики.

Данная работа посвящена анализу момента наступления редкого события (момента совершения ближайшей успешной атаки) на основе аппарата редких событий в регенерирующих неоднородных процессах. Работ по однородным регенерирующим процессам применительно к задачам анализа надежности систем достаточно много – перечень многих важных работ по данной тематике приведен в [2]. Результатов по использованию данного аппарата для анализа показателей ИБ найти не удалось. Работ, учитывающих неоднородность регенерирующего процесса, практически нет. Ранее авторами были опубликованы две работы по данной тематике [1, 5–7], являющиеся вспомогательными для основного результата данной работы – оценки момента первой успешной злоумышленной атаки.

Анализ асимптотического поведения момента ближайшей атаки

Введем необходимые обозначения и опишем ограничения. Полный анализ этих условий и анализ их содержания проведены в [1].

Пусть задан случайный процесс $\kappa(t)$, и $t_0 = 0 < t_1 < t_2 < \dots < t_n < \dots$ есть точки регенерации процесса $\kappa(t)$ (моменты времени совершения действий, связанных с нарушением ИБ). Предположим, что на каждом интервале $[t_{n-1}, t_n)$ в некоторый момент $t_{n-1} + \eta_n$ ($0 \leq \eta_n < \xi_n$) может произойти или не произойти некоторое событие A_n (в нашем случае – успешная атака, связанная с нарушением ИБ), причем событие A_n и величина η_n определены на классе траекторий $\{\kappa(t), t_{n-1} \leq t < t_n\}$ и, таким образом, не зависят от поведения процесса $\kappa(t)$ вне промежутка $[t_{n-1}, t_n)$. Пусть χ_k есть индикатор события A_k , τ_n – случайный момент первого после t_{n-1} появления одного из событий A_k ($k \geq n$); $\zeta_n \stackrel{\text{def}}{=} \xi_n(1 - \chi_n) + \eta_n \chi_n$. Введем следующие обозначения ($n \geq 1; z \geq 0$):

$$\varphi_n(z) = M(e^{-z\xi_n}); \overline{\varphi}_n(z) = 1 - \varphi_n(z); q_n = P\{\chi_n = 1\};$$

$$\varphi_n^-(z) = M(e^{-z\xi_n} \chi_n); \varphi_n^+(z) = M(e^{-z\xi_n} (1 - \chi_n)); \pi_n(z) = \overline{\varphi}_n(z) + \varphi_n^-(z),$$

где M – знак математического ожидания. Заметим, что $\overline{\varphi}_n(0) = 0$ и $\varphi_n^-(0) = q_n$.

В дальнейшем все введенные характеристики будут являться функциями некоторого параметра $\gamma \in \Theta$ (т. е. $q_n = q_n(\gamma)$, $\varphi_n^-(z) = \varphi_n^-(\gamma, z)$, $\pi_n(z) = \pi_n(\gamma, z)$ и т. д.), где Θ – некоторое множество на действительной прямой, для которого точка 0 является предельной точкой. Всюду ниже запись « $\gamma \rightarrow 0$ » означает, что $\gamma \rightarrow 0$ так, что $\gamma \in \Theta$.

Ниже приводятся и исследуются условия, наличие которых предполагается при доказательстве основных результатов. Вся совокупность условий разбивается на группы следующим образом.

А. Существуют функции $g_n(\gamma)$ и $m(\gamma)$ ($n \geq 1 - */ \gamma \in \Theta$) такие, что $\lim_{\gamma \rightarrow 0} m(\gamma) = \lim_{\gamma \rightarrow 0} g_n(\gamma) = 0$ и при любых $n \geq 1, z > 0$ существует предел

$$\lim_{\gamma \rightarrow 0} \{\overline{\varphi}_n(m(\gamma)z)g_n(\gamma)^{-1}\} \stackrel{def}{=} \omega_n(z), \quad \omega_n(1) = 1. \quad (1)$$

Б. Справедливо соотношение $\limsup_{\gamma \rightarrow 0} \lim_{n \geq 1} q_n(\gamma) = 0$.

Прежде чем описывать остальные условия, введем обозначения ($n \geq 1, \gamma > 0$):

$$S_1(n, \gamma) = \sum_{k=1}^n q_k(\gamma); \quad S_2(n, \gamma) = \sum_{k=1}^n g_k(\gamma).$$

Ниже часто для простоты вместо обозначения $S_i(n, \gamma)$ будет использовано обозначение $S_i(n)$.

В. Для любых $\gamma > 0$ и целых $n > 0$ справедливы соотношения

$$S_i(n) = n^{\theta_i} L_i(n) G_i(\gamma) (1 + \alpha_i(n, \gamma)), \quad i = \overline{1, 2}, \quad (2)$$

где $\theta_i \geq 0, L_i(x) (x > 0)$ – медленно меняющаяся функция, $\lim_{n \rightarrow \infty, \gamma \rightarrow 0} \alpha_i(n, \gamma) = 0$.

При этом [5] справедливы соотношения:

$$\lim_{\gamma \rightarrow 0} G_i(\gamma) = 0, \quad i = \overline{1, 2}.$$

Необходимо $\theta_2 \leq 1$ и $\lim_{\gamma \rightarrow 0} (\lambda_i(\gamma)) = +\infty$ для $i = 1, 2$. Положим $\lambda(\gamma) = \min(\lambda_1(\gamma), \lambda_2(\gamma))$.

Г. Существует предел:

$$\lim_{\gamma \rightarrow 0} (\lambda_1(\gamma) / \lambda_2(\gamma)) \stackrel{def}{=} \lambda_0, \quad 0 \leq \lambda_0 \leq +\infty.$$

Д. Для любого фиксированного $x > 0$ условие (1) выполняется равномерно по $n \leq x \lambda(\gamma)$, т. е.

$$\lim_{\gamma \rightarrow 0} \{ \max_{1 \leq n \leq x \lambda(\gamma)} \max |\overline{\varphi}_n(m(\gamma)z)(g_n(\gamma))^{-1} - \omega_n(z)| \} = 0.$$

Е. Равномерно по k и $x \in (a, b)$, где a и b ($0 < a < b < +\infty$) произвольные числа, для любого $T \geq 1$ имеют место соотношения

$$\lim_{\gamma \rightarrow 0} \{ \max_{1 \leq n \leq x \lambda(\gamma)} |\overline{\varphi}_n(m(\gamma)z)(g_n(\gamma))^{-1} - \omega_n(z)| \} = 0; \quad (3)$$

$$\lim_{\gamma \rightarrow 0} \sum_{m \in N_k, m \leq x \lambda(\gamma)} g_m(\gamma) \stackrel{def}{=} \mu_k(x), \quad (4)$$

где $Q_n(\gamma) = g_n(\gamma) + q_n(\gamma)$ ($n \geq 1$), при $|N_k| < +\infty$ полагаем $Q_n(\gamma) = 0$ для $n > |N_k|$; $\chi(A)$ есть индикатор события A ; множества N_k вводятся в утверждении леммы 2 [1].

Условие (3) можно заменить на следующее условие: для любого $T \geq 1$ равномерно по k ($1 \leq k \leq M$) и $x \in (a, b)$, где a и b ($0 < a < b < \infty$) – любые числа, существуют пределы:

$$\lim_{\gamma \rightarrow 0} \{ \sum_{k=1}^n Q_{i^{(k)}}(\gamma) (\sum_{m \in N_k, m \leq x \lambda(\gamma)} Q_{j^{(k)}}(\gamma))^{-1} \} = 0.$$

Вместо выполнения совокупности условий В и Г можно потребовать выполнение следующих более общих условий В' и Г'.

В'. Существует функция $\lambda(\gamma)$ ($\gamma > 0$) такая, что для любого $x > 0$ существуют пределы ($i = 1, 2$):

$$\lim_{\gamma \rightarrow 0} S_i(x \lambda(\gamma)) \stackrel{def}{=} \sigma_i(x) < +\infty, \quad \max(\sigma_1(x), \sigma_2(x)) \neq 0.$$

Г'. Существуют функции $\varphi_1(x), \varphi_2(x)$ ($x > 0$) и числа $\gamma_0, A > 0$ такие, что для всех $x > A$ и $i = 1, 2; j = 3, 5$:

$$\inf_{|\gamma| \leq \gamma_0} |S_i(x \lambda(\gamma))| \geq \vartheta_1(x); \quad \sup_{|\gamma| \leq \gamma_0} |S_i(x \lambda(\gamma))| \leq \vartheta_2(x),$$

причем для любого $P < 1$

$$\int_A e^{-P\varphi_1(y)} d\varphi_2(y) < \infty.$$

Из условия В' следует $\lim_{\gamma \rightarrow 0} \lambda(\gamma) = +\infty$. Справедливы соотношения ($x > 0$):

$$\sum_{k=1}^{\infty} \mu_k(x) = \sigma_2(x).$$

Можно считать, что функции $\vartheta_1(y)$ и $\vartheta_2(y)$ монотонно не убывают с ростом y .

Теорема. Пусть выполнены условия А, Б, В', Г', Д и Е. Тогда существует предел

$$Me^{-m(\gamma)\tau_1} = \int_0^{\infty} \sigma_1(y) d_y (1 - \exp\{-\sum_{k=1}^M \psi_k(z)\mu_k(y) - \sigma_1(y)\}).$$

Доказательство. Положим, $a_n(z) = Me^{-z\tau_n}$ ($n \geq 1, z > 0$). Имеем:

$$a_n(z) = \varphi_n^-(z) + \varphi_n^+(z)a_{n+1}(z) = \dots = \sum \prod \varphi_{n+l-1}^+(z)\varphi_{n+k-1}^-(z), \quad (5)$$

откуда следует:

$$a_1(z) = \sum_{k=1}^{\infty} \prod_{l=1}^{k-1} (1 - \overline{\varphi}_l(z) - \varphi_l^-(z))\varphi_k^-(z). \quad (6)$$

Рассмотрим независимые случайные величины (СВ) $\{v = \nu(z), \xi_k, k \geq 1\}$ со следующими распределениями ($k \geq 1, z > 0$):

$$P(\xi_k = 1) = \overline{\varphi}_k(z); P(\xi_k = -1) = \varphi_k^-(z); P(\xi_k = 0) = 1 - \pi_k(z);$$

$$P(v = n) = \prod_{l=1}^{n-1} (1 - \pi_l(z))\pi_n(z).$$

Из определения СВ v имеем $P(v = k) = \prod_{i=1}^{k-1} (1 - \pi_i(z)) - \prod_{i=1}^k (1 - \pi_i(z))$, откуда следует, что

$P(v \geq k) = \prod_{i=1}^{k-1} (1 - \pi_i(z))$ и справедливо соотношение

$$a_1(z) = \sum_{k=1}^{\infty} \varphi_k^-(z)P(v \geq k). \quad (7)$$

Покажем вначале, что равномерно по $x \in (a, b)$ ($0 < a < b < \infty$) справедливо соотношение ($z > 0$), где $\lim_{\gamma \rightarrow 0} \alpha(\gamma) = 0$ равномерно по $x \leq x_0\lambda(\gamma)$ (см. Д и лемму 3 [5]), x_0 – любое число, а множества N_k ($k \geq 1$) вводятся в лемме 1 [5] и условии Е.

При данном фиксированном $\varepsilon > 0$ выберем $\mu \geq 1$ так, чтобы для всех $n > \mu$ и $k \geq 1$ имели z (см. условие Е):

$$\lim_{\gamma \rightarrow 0} \sum_{1 \leq k \leq x\lambda(\gamma)} \pi_k(m(\gamma)z) = \sum_{k=1}^M \psi_k(z)\mu_k(x) + \sigma_1(x). \quad (8)$$

В силу условий А, Д и леммы 1 [1] имеем: при $\gamma \rightarrow 0$ ($z > 0$)

$$\begin{aligned} \sum_{1 \leq k \leq x\lambda(\gamma)} \pi_k(m(\gamma)z) &= \sum_{k=1}^M \sum_{\substack{l \in N_k \\ l \leq x\lambda(\gamma)}} \left(\frac{\overline{\varphi}_k(m(\gamma)z)}{g_l(\gamma)} g_l(\gamma) + \frac{\varphi_k^-(m(\gamma)z)}{q_l(\gamma)} q_l(\gamma) \right) = \\ &= \left\{ \sum_{k=1}^M \sum_{\substack{l \in N_k \\ l \leq x\lambda(\gamma)}} \omega_l(z) g_l(\gamma) + S_1(x\lambda(\gamma)) \right\} (1 + \alpha(\gamma)). \end{aligned} \quad (9)$$

Имеем: $|\omega_{i_n^{(k)}}(z) - \psi_k(z)| \leq \varepsilon$, на основе чего выводим следующие оценки:

$$\begin{aligned} \left| \sum_{k=1}^M \sum_{\substack{l \in N_k \\ l \leq x\lambda(\gamma)}} (\omega_l(z) - \psi_k(z)) g_l(\gamma) \right| &\leq \sum_{k=1}^M \sum_{j=1}^{\mu} [\max(|\omega_l(z)|, |\psi_k(z)|)] g_{i_j^{(k)}}(\gamma) \times \\ &\times \chi(i_j^{(k)} \leq x\lambda(\gamma)) + \varepsilon \sum_{k=1}^M \sum_{j=\mu+1}^{\infty} g_{i_j^{(k)}}(\gamma) \cdot \chi(i_j^{(k)} \leq x\lambda(\gamma)) \leq \\ &\leq |\max(1, z) - \varepsilon| \cdot \left(\sum_{k=1}^M \sum_{j=1}^{\mu} g_{i_j^{(k)}}(\gamma) + \varepsilon \sum_{\substack{l \in N_k \\ l \leq x\lambda(\gamma)}} g_l(\gamma) \right), \end{aligned}$$

где мы воспользовались тем, что при $z < 1$ $\infty \leftarrow l(z) < \infty \leftarrow l(1) = 1$ и $\psi_k(z) < \psi_k(1) = 1$, а при $z > 1$, в силу выпуклости вниз функций $\omega \leftarrow l(z)$ ($l \geq 1$) и $\psi \leftarrow k(z)$ ($k \geq 1$) (как пределов выпуклых вниз функций $\varphi_n(z)$ и $\omega \leftarrow l(z)$ соответственно) и условий $\omega \leftarrow l(0) = \psi \leftarrow l(0) = 0$ и $\omega \leftarrow l(1) = \psi \leftarrow l(1) = 1$, справедливы неравенства $\omega_l(z) < z$, $\psi_k(z) < z$. Отсюда, в силу (10) [1] и первого соотношения в (11) [1], переходя вначале к пределу при $\gamma \rightarrow 0$, затем при $\varepsilon \rightarrow 0$, получаем:

$$\lim_{\gamma \rightarrow 0} \sum_{k=1}^M \sum_{\substack{l \in N_k \\ l \leq x\lambda(\gamma)}} (\omega_l(z) - \psi_k(z)) g_l(\gamma) = 0.$$

Из (5)–(7), (9), условия В' и (2) следует (8).

Далее, имеем ($y > 0$):

$$\begin{aligned} P(v(m(\gamma)z) \geq y) &= \prod_{0 < l \leq y} (1 - \pi_l(m(\gamma)z)) = \\ &= \exp \left\{ - \sum_{0 < l \leq y} \pi_l(m(\gamma)z) (1 + O(\max_{0 < l \leq y} \pi_l(m(\gamma)z))) \right\}. \end{aligned} \quad (10)$$

Воспользовавшись тем, что функция $\overline{\varphi}_n(z)$ монотонно возрастает, а функция $\overline{\varphi}_n(z)/z$ монотонно убывает, нетрудно получить соотношения

$$\min(1, z) \overline{\varphi}_n(m(\gamma)) \leq \overline{\varphi}_n(m(\gamma)z) \leq \max(1, z) \overline{\varphi}_n(m(\gamma)),$$

на основе чего, используя условие Д и (2) [5], получаем ($l \geq 1$):

$$\pi_l(m(\gamma)z) \leq \max(1, z) \sup_{l \geq 1} \frac{\overline{\varphi}_l(m(\gamma))}{g_l(\gamma)} g_l(\gamma) + \sup_{l \geq 1} \frac{\varphi_l^-(m(\gamma)z)}{q_l(\gamma)} q_l(\gamma) \rightarrow 0 \quad (11)$$

при $\gamma \rightarrow 0$ равномерно по $l \geq 1$.

Из (8), (10) и (11) выводим: равномерно по $y \leq x$ при $\gamma \rightarrow 0$

$$\begin{aligned} P(v(z) \geq y\lambda(\gamma)) &= \exp \left\{ - \sum_{0 < l \leq y\lambda(\gamma)} \pi_l(m(\gamma)z) (1 + O(\max_{0 < j \leq y\lambda(\gamma)} \pi_j(m(\gamma)z))) \right\} = \\ &= \exp \left\{ - \sum_{k=1}^M \psi_k(z) \mu_k(y) - \sigma_1(y) \right\} (1 + o(1)). \end{aligned} \quad (12)$$

Исследуем асимптотическое поведение при $\gamma \rightarrow 0$ функции $a_1(z)$.

Имеем:

$$\begin{aligned} a_1(z) &= \int_0^{\infty} P(v(m(\gamma)z) \geq y) d_y \sum_{0 < n \leq y} \varphi_n^-(m(\gamma)z) = \\ &= \int_0^{\infty} P(v(m(\gamma)z) \geq y\lambda(\gamma)) d_y \sum_{0 < n \leq y\lambda(\gamma)} \varphi_n^-(m(\gamma)z). \end{aligned} \quad (13)$$

Выберем $\gamma_0 > 0$ так, чтобы при $|\gamma| < \gamma_0$ в (10) выражение $1 + O(\max_{1 \leq l \leq y} \pi_l(m(\gamma)z))$ было не меньше $1/2$ равномерно по $y > 0$; последнее возможно в силу (11). Тогда, воспользовавшись (11) и (13), получаем: при $|\gamma| < \gamma_0$

$$\begin{aligned} P(v(m(\gamma)z) \geq y) \sum_{0 < n \leq y} \pi_n(m(\gamma)z) &\leq \exp\left\{-\frac{1}{2} \sum_{0 < n \leq y} (\pi_n(m(\gamma)z))\right\} \times \\ &\times \sum_{0 < n \leq y} \pi_n(m(\gamma)z) \rightarrow 0 \text{ при } y \rightarrow \infty, \end{aligned} \quad (14)$$

поскольку $\sum_{0 < n \leq y} (\pi_n(m(\gamma)z)) > \inf_{n > 0} \frac{\varphi_n^-(m(\gamma)z)}{q_n(\gamma)} S_1(y)$; $\lim_{y \rightarrow \infty} S_1(y) \rightarrow +\infty$ (в силу условия Б),

$\inf_{n > 0} \frac{\varphi_n^-(m(\gamma)z)}{q_n(\gamma)} > 0$ в силу (1) [6] и $\lim_{a \rightarrow \infty} (e^{-(1/2)a} a) = 0$.

Из (12) и неравенств $\varphi_n^-(z) \leq \pi_n(z)$ ($n \geq 1$) получаем:

$$\lim_{y \rightarrow \infty} \{P(v(m(\gamma)z) \geq y\lambda(\gamma)) \sum_{0 < n \leq y\lambda(\gamma)} \varphi_n^-(m(\gamma)z)\} = 0,$$

на основе чего после интегрирования по частям в (11) [1] выводим

$$a_1(z) = \int_0^{\infty} \sum_{0 < n \leq y\lambda(\gamma)} \varphi_n^-(m(\gamma)z) d_y (1 - P(v(m(\gamma)z) \geq y\lambda(\gamma))). \quad (15)$$

Положим ($0 \leq a < b \leq \infty$):

$$J(a, b) \stackrel{\text{def}}{=} \int_a^b \sum_{0 < n \leq y\lambda(\gamma)} \varphi_n^-(m(\gamma)z) d_y P(v(m(\gamma)z) < y\lambda(\gamma)).$$

Заметим, что из (8) [1] следует: для всех $n \geq 1$

$$\omega_n(z) = \lim_{\gamma \rightarrow 0} \frac{\overline{\varphi}_n(m(\gamma)z)}{g_n(\gamma)} \leq \max(1, z) \lim_{\gamma \rightarrow 0} \frac{\overline{\varphi}_n(m(\gamma))}{g_n(\gamma)} = \max(1, z) \omega_n(1) = \max(1, z),$$

откуда выводим: $\psi_k(z) \leq \max(1, z)$ для всех $k \geq 1$.

Из леммы 1 [5] следует: существует функция $K(z)$, не зависящая от γ , и константа γ_1 такие, что $\frac{\overline{\varphi}_n(m(\gamma)z)}{q_n(\gamma)} \leq K(z)$ для всех $n > 0$ и $\gamma < \gamma_1$. На основе последнего неравенства получаем: для любого $\varepsilon > 0$, в силу (12), условия В' и (6), имеем

$$\begin{aligned} \overline{\lim}_{\gamma \rightarrow 0} J(0, \varepsilon) &\leq K(z) \overline{\lim}_{\gamma \rightarrow 0} \{S_1(\varepsilon\lambda(\gamma)) P(v(m(\gamma)z) < \varepsilon\lambda(\gamma))\} \leq \\ &\leq K(z) \sigma_1(\varepsilon) (1 - \exp\{-\sum_{k=1}^M \psi_k(z) \mu_k(\varepsilon) - \sigma_1(\varepsilon)\}), \end{aligned} \quad (16)$$

откуда, ввиду первого соотношения в (16) и неравенства $1 - e^{-a} \leq a$ ($a \geq 0$), выводим: при $\varepsilon \rightarrow 0$

$$\begin{aligned} \overline{\lim}_{\gamma \rightarrow 0} J(0, \varepsilon) &\leq K(z) \sigma_1(\varepsilon) \left(\sum_{k=1}^M \psi_k(z) \mu_k(\varepsilon) + \sigma_1(\varepsilon) \right) \leq \\ &\leq K(z) \sigma_1(\varepsilon) (\max(1, z) \sigma_2(\varepsilon) + \sigma_1(\varepsilon)) = O(\sigma_1(\varepsilon) \max_{i=1,2} \sigma_i(\varepsilon)). \end{aligned} \quad (17)$$

Совершенно так же, как и при выводе (13), на основе (10) доказывается существование константы $\gamma_2 > 0$, $\gamma_2 \leq \max(\gamma_0, \gamma_1)$, такой, что для всех $\gamma (|\gamma| < \gamma_2)$ и $l \geq 1$

$$\begin{aligned} \pi_l(m(\gamma)z) &\geq \min(1, z) \inf_{l \geq 1} \frac{\overline{\Phi}_l(m(\gamma))}{g_l(\gamma)} g_l(\gamma) + \inf_{l \geq 1} \frac{\overline{\Phi}_l(m(\gamma)z)}{q_l(\gamma)} q_l(\gamma) \geq \\ &\geq P_1 q_n(\gamma) + P_2 g_n(\gamma), \end{aligned} \quad (18)$$

где, в силу (4) [6] и условия Д,

$$\begin{aligned} P_1 &\stackrel{\text{def}}{=} \inf_{|\gamma| < \gamma_1} \inf_{n \geq 1} \frac{\overline{\Phi}_n(m(\gamma)z)}{q_n(\gamma)} > 0; \\ P_2 &\stackrel{\text{def}}{=} \min(1, z) \inf_{|\gamma| < \gamma_1} \inf_{n \geq 1} \frac{\overline{\Phi}_n(m(\gamma))}{g_n(\gamma)} \geq 0. \end{aligned}$$

Заметим, что, в силу (1) [5], выбрав γ_2 достаточно малым, можно сделать P_1 сколь угодно близким к единице, поэтому при достаточно малых γ величина $\max(P_1, P_2)$ сколь угодно близка к единице.

Из (18), аналогично выводу (14), получаем: при $|\gamma| < \gamma_2$ для всех $y > 0$

$$P(v(m(\gamma)z)) \geq y \leq \exp\{-P_1 S_1(y)/2 - P_2 S_2(y)/2\}. \quad (19)$$

Далее, для любого $A > \varepsilon$, аналогично (18), на основе первого условия Γ' получаем:

$$\begin{aligned} \overline{\lim}_{\gamma \rightarrow 0} J(A, \infty) &\leq K(z) \overline{\lim}_{\gamma \rightarrow 0} \int_A^\infty S_2(y \lambda(\gamma)) d_y P(v(m(\gamma)z) < y \lambda(\gamma)) \leq \\ &\leq K(z) \overline{\lim}_{\gamma \rightarrow 0} \int_A^\infty \vartheta_2(y) d_y P(v(m(\gamma)z) < y \lambda(\gamma)). \end{aligned} \quad (20)$$

В силу (19), условия Γ' и неравенства $P_1 S_1(y) + P_2 S_2(y) \geq (P_1 + P_2) \min(S_1(y), S_2(y))$ имеем $(P(P_1 + P_2)/2)$:

$$\begin{aligned} P\{v(m(\gamma)z) \geq A \lambda(\gamma)\} \vartheta_2(A) &\leq \\ &\leq \exp\{-P \min(S_1(A \lambda(\gamma)), S_2(A \lambda(\gamma)))\} \vartheta_2(A) \leq \exp\{-P \vartheta_1(A)\} \vartheta_2(A). \end{aligned} \quad (21)$$

Из (20), (21) после интегрирования по частям на основе условия Γ' окончательно получаем:

$$\begin{aligned} \overline{\lim}_{\gamma \rightarrow 0} J(A, \infty) &\leq K(z) \left\{ \overline{\lim}_{\gamma \rightarrow 0} P(v(m(\gamma)z) \geq A \lambda(\gamma)) \vartheta_2(A) + \int_A^\infty P(v(m(\gamma)z) \geq y \lambda(\gamma)) d \vartheta_2(y) \right\} \leq \\ &\leq K(z) \left\{ \exp(-P \vartheta_1(A)) + \int_A^\infty \exp(-P \vartheta_1(y)) d \vartheta_2(y) \right\}. \end{aligned} \quad (22)$$

Совершенно так же, как и выше, при доказательстве (10) на основе леммы 1 [5], показывается, что

$$\sum_{1 \leq k \leq y \lambda(\gamma)} \overline{\Phi}_k(m(\gamma)z) = \sum_{k \leq y \lambda(\gamma)} \left(\frac{\overline{\Phi}_k(m(\gamma)z)}{q_k(\gamma)} \right) q_k(\gamma) = \sum_{k \leq y \lambda(\gamma)} q_k(\gamma) (1 + \alpha_0(\gamma)) = S_1(y \lambda(\gamma)) (1 + \alpha_0(\gamma)), \quad (23)$$

где $\lim_{\gamma \rightarrow 0} \alpha_0(\gamma) = 0$ равномерно по $y \in (\varepsilon, A)$. Из (23), ввиду условия В', выводим: равномерно по $y \in (\varepsilon, A)$

$$\lim_{\gamma \rightarrow 0} \sum_{1 \leq k \leq y \lambda(\gamma)} \overline{\Phi}_k(m(\gamma)z) = \sigma_1(y). \quad (24)$$

Поскольку $a_1(z) = J(0, \varepsilon) + J(\varepsilon, A) + J(A, \infty)$, и в силу (15)

$$\lim_{A \rightarrow \infty} \int_A^\infty e^{-P\vartheta_1(y)} d\vartheta_2(y) = 0,$$

то из (17), (22) и (24) окончательно получаем:

$$\begin{aligned} \lim_{\gamma \rightarrow 0} a_1(z) &= \int_\varepsilon^A \sigma_1(y) d_y [1 - \exp\{-\sum_{k=1}^M \psi_k(z) \mu_k(y) - \sigma_1(y)\}] + \\ &+ O(\sigma_1(\varepsilon) \max(\sigma_1(\varepsilon), \sigma_2(\varepsilon))) + o_A(1) \text{ при } \varepsilon \rightarrow 0, A \rightarrow \infty. \end{aligned}$$

Аналогичное соотношение имеет место и для $\overline{\lim}_{\gamma \rightarrow 0} a_1(z)$, что после перехода к пределу при $\varepsilon \rightarrow 0$ и $A \rightarrow \infty$ дает (при $\gamma \rightarrow 0$)

$$a_1(z) = \int_0^\infty \sigma_1(y) d_y (1 - \exp\{-\sum_{k=1}^M \psi_k(z) \mu_k(y) - \sigma_1(y)\}).$$

Следствие 1. Пусть выполнены условия А, Б, В, Г, Д и Е. Тогда справедливо утверждение теоремы с $\sigma_1(y) = \min(1, \lambda_0^{-\theta_1}) y^{\theta_1}$.

Доказательство следует из лемм 1 и 2 [5] и теоремы.

Пример типовой модели

Приведем важный пример использования доказанной теоремы.

Пусть последовательность СВ ζ_n стареет с интенсивностью n^β , т. е. функция распределения (ФР) $F_n(t)$ случайной величины ζ_n равна $F_n(t) = F(t/n^\beta)$ ($n \geq 1, \beta > -1/\alpha$), где $F(t)$ ($F(-0) = 0$) – заданная ФР такая, что при $t \rightarrow \infty \cdot 1 - F(t) \sim C \cdot t^{-\alpha}$, $0 < \alpha < 1$ и C – некоторая константа. Далее, $q_n(\gamma) = \min(1, K_n(\gamma) \gamma^\delta n^\tau)$ ($\delta > 0, -1 < \tau \leq 0$), где $\Gamma(x)$ – гамма-функция Эйлера, $\lim_{\gamma \rightarrow 0} K_n(\gamma) = K_n$

равномерно по $n \geq 1$ и $\lim_{n \rightarrow \infty} K_n = K$. Положим: $m(\gamma) = \gamma$, $g_n(\gamma) = C(\Gamma(\alpha))^{-1} (\gamma n^\beta)^\alpha$, $\varphi(z) = \int_0^\infty e^{-zt} dF(t)$.

Тогда $0 < K < +\infty$, $\varphi_n(z) = \varphi(zn^\beta)$.

В силу условий на ФР $F(t)$ и тауберовых теорем имеем:

$$\varphi(z) \sim 1 - C(\Gamma(\alpha))^{-1} z^\alpha \text{ при } z \downarrow 0,$$

на основе чего получаем: при $\gamma \rightarrow 0$ и фиксированном $n \geq 1$

$$\frac{1 - \varphi_n(\gamma z)}{g_n(\gamma)} = \frac{1 - \varphi(\gamma n^\beta z)}{(\gamma n^\beta)^\alpha C(\Gamma(\alpha))^{-1}} \rightarrow z^\alpha,$$

т. е. $\omega_n(z) = z^\alpha$ для всех $n \geq 1$ и, значит, выполнены условия А.

Так как сходимость $\lim_{\gamma \rightarrow 0} K_n(\gamma) = K_n$ имеет место равномерно по $n \geq 1$, то при достаточно малых γ последовательность $\{K_n(\gamma), n \geq 1\}$ (а значит, и последовательность $\{K_n, n \geq 1\}$) равномерно по n ограничена. Отсюда, ввиду оценки $q_n(\gamma) \leq K_n(\gamma) \gamma^\delta n^\tau$, следует, что $q_n(\gamma)$ стремится к нулю при $n \rightarrow \infty$ равномерно по $n \geq 1$, т. е. выполнено условие Б.

Пользуясь соотношением ($\theta > -1$): $\sum_{m=1}^n K_m(\gamma) m^\theta \sim \int_1^n K_{[x]}(\gamma) x^\theta dx$ при $n \rightarrow \infty$

и $\int_1^n K_{[x]}(\gamma) x^\theta dx - \int_1^n K(\gamma) x^\theta dx = o_\gamma(\int_1^n x^\theta dx)$ при $\gamma \rightarrow 0$, выводим: при $n \rightarrow \infty$ и $\gamma \rightarrow 0$

$$\sum_{m=1}^n K_m(\gamma) m^\theta \sim K(\theta + 1)^{-1} n^{\theta+1}$$

и, следовательно,

$$S_1(n) = \sum_{m=1}^n \min(1, K_m(\gamma)\gamma^\delta m^\tau) = \sum_{m=1}^n K_m(\gamma)\gamma^\delta m^\tau + n_0 - \sum_{m=1}^{n_0} K_m(\gamma)\gamma^\delta m^\tau \sim \gamma^\delta K(\tau+1)^{-1} n^{\tau+1} + O(1) \sim \gamma^\delta K(\tau+1)^{-1} n^{\tau+1}, \quad (25)$$

где $n_0 \geq 0$ есть наибольшее n такое, что $q_n(\gamma) = 1$. Далее, аналогично

$$S_2(n) = \sum_{m=1}^n (C(\Gamma(\alpha))^{-1} \gamma n^\beta)^\alpha = (C(\Gamma(\alpha)))^{-1} \gamma^\alpha \sum_{m=1}^n m^{\beta\alpha} \sim (C(\Gamma(\alpha)))^{-1} \gamma^\alpha \frac{n^{\beta\alpha+1}}{\beta\alpha+1}. \quad (26)$$

Из (25), (26) следует выполнение условия В.

Функции $\lambda_1(\gamma)$ и $\lambda_2(\gamma)$ (см. лемму 1 [1]) могут быть найдены из соотношений $\gamma^\delta K(\tau+1)^{-1} (\lambda_1(\gamma))^{\tau+1} = 1$ и $C(\Gamma(\alpha))^{-1} \gamma^\alpha \frac{(\lambda_2(\gamma))^{\beta\alpha+1}}{\beta\alpha+1} = 1$, т. е. $(\lambda_1(\gamma))^{\tau+1} = \gamma^{-\delta} K^{-1}(\tau+1)$ и $\lambda_2(\gamma) = (C^{-1}\Gamma(\alpha)(\beta\alpha+1))^{\frac{1}{\beta\alpha+1}} \gamma^{\frac{\alpha}{\beta\alpha+1}}$.

Отсюда следует выполнение условия Г с

$$\lambda_0 = \begin{cases} \frac{K\Gamma(\alpha)(\beta\alpha+1)^{\frac{1}{\beta\alpha+1}}}{C(\tau+1)^{\frac{1}{\tau+1}}}, & \text{Н}^-\text{Ц } \delta = \frac{\alpha}{\beta\alpha+1}, \\ 0 & \text{Н}^-\text{Ц } \delta < \frac{\alpha}{\beta\alpha+1}, \\ \infty & \text{Н}^-\text{Ц } \delta > \frac{\alpha}{\beta\alpha+1}, \end{cases}$$

а также справедливость соотношения $\lambda(\gamma) = \min\{(C^{-1}\Gamma(\alpha)(\beta\alpha+1))^{\frac{1}{\beta\alpha+1}} \gamma^{\frac{\alpha}{\beta\alpha+1}}; (K^{-1}(\tau+1))^{\frac{1}{\tau+1}} \gamma^{\frac{\delta}{\tau+1}}\}$.

Поскольку $\lim_{\gamma \rightarrow 0} \{(\gamma^{-\frac{\alpha}{\beta\alpha+1}})^\beta \gamma\} = 0$, то, в силу (20), $\lim_{\gamma \rightarrow 0} \{(\lambda(\gamma))^\beta \gamma\} = 0$ и для любого $x > 0$ $\lim_{\gamma \rightarrow 0} \max_{1 \leq n \leq x\lambda(\gamma)} (\gamma n^\beta) = 0$. Отсюда следует, что соотношение (25) имеет место равномерно по $n \leq x\lambda(\gamma)$, т. е. выполнено предельное соотношение условия Д.

Наконец, выполнение условия Е следует из того, что $M = 1$. При этом, в силу (16), $\mu_1(x) = m_2 x^{\theta_2}$.

Таким образом, мы показали справедливость условий А–Е, что, в силу следствия 1, влечет следующее соотношение:

$$\begin{aligned} \lim_{\gamma \rightarrow 0} M e^{-s\gamma^\tau} &= -\int_0^\infty m_1 y^{\theta_1} d_y \exp\{-z^\alpha m_2 y^{\theta_2} - m_1 y^{\theta_1}\} = \\ &= m_1 \int_0^\infty y^{\theta_1} (\theta_2 m_2 z^\alpha y^{\theta_2} + \theta_1 m_1 y^{\theta_1}) \exp\{-z^\alpha m_2 y^{\theta_2} - m_1 y^{\theta_1}\} dy. \end{aligned}$$

Заключение

В работе проводится анализ модели, описывающей процесс атак на защищаемый объект, где хранится закрытая информация, построенной на основе аппарата регенерирующих последовательностей успешного завершения злонамеренных атак. Именно, моменты реализации атак рассматриваются как точки регенерации атак. Предполагается, что атаки, исходящие из одного источника, происходят достаточно редко, т. е. событие успешного совершения атаки является редким событием, но потери при ее успешном завершении могут быть огромными. В качестве исследуемой характеристики выбран ближайший момент, когда очередная атака, которая является одной из наиболее важных с точки зрения информационной безопасности, окажется успешной.

Исследования проводятся при предположении неоднородности всех характеристик модели, что более адекватно соответствует реальному состоянию в системах информационной безопасности.

В работе получено асимптотическое соотношение для момента совершения ближайшей успешной злонамеренной атаки в условиях, когда интервал времени, на котором проводится анализ атак, неограниченно растет, и одновременно вероятности совершения атак становятся все более редкими, причем эти величины изменяются согласованным образом. Необходимо уточнить данный результат применительно к конкретным типам объектов защиты и конкретным условиям их функционирования, что предполагается сделать в последующих работах авторов.

СПИСОК ЛИТЕРАТУРЫ

1. Попов Г. А., Попов А. Г., Лантев П. В. Формализация процесса изменения вероятности нарушения сервисов информационной безопасности на основе аппарата редких событий // Наука, образование, инновации: пути развития: сб. материалов VIII Всерос. науч.-практ. конф. (Петропавловск-Камчатский, 23–25 мая 2017 г.). Петропавловск-Камчатский: Изд-во КамчатГТУ, 2017. С. 29–34.
2. Гнеденко Д. Б., Соловьев А. Д. Одна общая модель резервирования с восстановлением // Изв. АН СССР. Техническая кибернетика. 1974. № 6. С. 113–119.
3. Гнеденко Д. Б., Соловьев А. Д. Асимптотическая оценка надежности сложных систем с быстрым восстановлением // Тр. III Всесоюз. школы-совещания по теории массового обслуживания. М.: Изд-во МГУ, 1975. Т. 1. С. 185–197.
4. Соловьев А. Д. Асимптотическое поведение момента первого наступления редкого события в регенерирующем процессе // Изв. АН СССР. Техническая кибернетика. 1971. № 6. С. 79–90.
5. Попов Г. А., Попова Е. А., Васильева О. В. Анализ входных условий в модели информационной безопасности, построенной на основе аппарата редких событий // Науч. вестн. Новосиб. гос. техн. ун-та. 2019. Т. 75. № 2. С. 69–88.
6. Попов Г. А. Асимптотическое поведение момента первого наступления редкого события в неоднородном регенерирующем процессе. М., 2000. 46 с.

Статья поступила в редакцию 24.12.2019

ИНФОРМАЦИЯ ОБ АВТОРАХ

Попов Георгий Александрович – Россия, 414056, Астрахань; Астраханский государственный технический университет; д-р техн. наук, профессор; зав. кафедрой информационной безопасности; popov@astu.org.

Попова Екатерина Александровна – Россия, 414056, Астрахань; Астраханский государственный технический университет; старший преподаватель кафедры информационной безопасности; e.popova@astu.org.



ANALYSIS OF TIME OF COMMITTING NEAREST MALICIOUS ATTACK IN INFORMATION SECURITY SYSTEM USING APPARATUS OF RARE REGENERATING PROCESSES

G. A. Popov, E. A. Popova

*Astrakhan State Technical University,
Astrakhan, Russian Federation*

Abstract. The paper analyzes the model that describes the process of attacking the protected object, where closed information is stored, the model built on the basis of the apparatus of regenerating sequences of the successful completion of malicious attacks. The moments of the attacks are considered in detail. It is assumed that attacks originating from a single source are rare enough, have an isolated singled character and are quite distant in time, that is, the event of a successful attack is a rare event, but the losses upon its successful completion can be huge. For the studied characteristic there is chosen a nearest moment when the next attack is successful: this characteris-

tic is very important with relation to the information security. Knowing the parameters of this characteristic will help, at appropriate time intervals, to take additional actions that increase the level of protection. Studies are conducted under the assumption that all characteristics of the model are heterogeneous, which more adequately corresponds to the real state in information security systems. There has been obtained an asymptotic relation for the moment of the next successful malicious attack under conditions when the time interval for analyzing the attack is constantly rising and the probability of attack is becoming less common, both values changing consistently.

Key words: information security, protected object, moment of nearest successful attack, regenerative processes, rare events.

For citation: Popov G. A., Popova E. A. Analysis of time of committing nearest malicious attack in information security system using apparatus of rare regenerating processes. *Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*. 2020;2:34-44. (In Russ.) DOI: 10.24143/2072-9502-2020-2-34-44.

REFERENCES

1. Popov G. A., Popov A. G., Laptev P. V. Formalizatsiia protsessa izmeneniia veroiatnosti narusheniia servisov informatsionnoi bezopasnosti na osnove apparata redkikh sobytii [Formalization of process of changing probability of violation of information security services based on apparatus of rare events]. *Nauka, obrazovanie, innovatsii: puti razvitiia: sbornik materialov VIII Vserossiiskoi nauchno-prakticheskoi konferentsii (Petropavlovsk-Kamchatskii, 23–25 maia 2017 g.)*. Petropavlovsk-Kamchatskii, Izd-vo KamchatGTU, 2017. Pp. 29-34.
2. Gnedenko D. B., Solov'ev A. D. Odnа obshchaia model' rezervirovaniia s vosstanovleniem [One common redundant backup model]. *Izvestiia AN SSSR. Tekhnicheskaiа kibernetika*, 1974, no. 6, pp. 113-119.
3. Gnedenko D. B., Solov'ev A. D. Asimptoticheskaiа otsenka nadezhnosti slozhnykh sistem s bystrym vosstanovleniem [Asymptotic reliability assessment of complex systems with fast recovery]. *Trudy III Vsesoiuznoi shkoly-soveshchaniia po teorii massovogo obsluzhivaniia*. Moscow, Izd-vo MGU, 1975. Vol. 1. Pp. 185-197.
4. Solov'ev A. D. Asimptoticheskoe povedenie momenta pervogo nastupleniia redkogo sobytiia v regeneriruiushchem protsesse [Asymptotic behavior of moment of first occurrence of rare event in regenerative process]. *Izvestiia AN SSSR. Tekhnicheskaiа kibernetika*, 1971, no. 6, pp. 79-90.
5. Popov G. A., Popova E. A., Vasil'eva O. V. Analiz vkhodnykh uslovii v modeli informatsionnoi bezopasnosti, postroennoi na osnove apparata redkikh sobytii [Analysis of input conditions in information security model built on apparatus of rare events]. *Nauchnyi vestnik Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta*, 2019, vol. 75, no. 2, pp. 69-88.
6. Popov G. A. Asimptoticheskoe povedenie momenta pervogo nastupleniia redkogo sobytiia v neodnorodnom regeneriruiushchem protsesse [Asymptotic behavior of moment of first occurrence of rare event in heterogeneous regenerative process]. Moscow, 2000. 46 p.

The article submitted to the editors 24.12.2019

INFORMATION ABOUT THE AUTHORS

Popov Georgiy Aleksandrovich – Russia, 414056, Astrakhan; Astrakhan State Technical University; Doctor of Technical Sciences, Professor; Head of the Department of Information Security; popov@astu.org.

Popova Ekaterina Aleksandrovna – Russia, 414056, Astrakhan; Astrakhan State Technical University; Senior Lecturer of the Department of Information Security; e.popova@astu.org.

