УДК 004.056.53

ТЕОРЕТИЧЕСКОЕ РАЗВИТИЕ МОДЕЛЕЙ ДЛЯ ОЦЕНКИ ЗАЩИЩЕННОСТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И СОХРАНЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИСПОЛЬЗУЕМОЙ ИНФОРМАЦИИ

Гусев К. В., Леонтьев А.С.

МИРЭА – «Российский технологический университет», 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail: leyla1542@rambler.ru, poltorak@mirea.ru

Рассмотрены вопросы использования аналитических моделей для оценки защищенности от НСД и сохранения конфиденциальности информации. На основе методов теории восстановления и аппроксимации используемых функций распределения двухпараметрическими распределениями разработан математический аппарат для оценки защищенности информации от несанкционированного доступа. Предложенные теоретические положения по оценке защищенности расширяют известные стандартизованные методы расчета, использующие однопараметрическую аппроксимацию функций распределения, являются достаточно универсальными и могут быть полезны широкому кругу специалистов.

Ключевые слова: модели, стандарт, рекомендации, конфиденциальность, защита информации, процессы восстановления, функция распределения, аппроксимация, несанкционированный доступ.

THEORETICAL DEVELOPMENT OF MODELS FOR THE ASSESSMENT OF SECURITY AGAINST UNAUTHORIZED ACCESS AND PRESERVATION OF THE CONFIDENTIALITY OF THE INFORMATION USED

Gusev K.V., Leontiev A.S.

MIREA - Russian Technological University, 119454, Moscow, 78 Vernadskogo Avenue, Russia, e-mail: leyla1542@rambler.ru, poltorak@mirea.ru

The issues of using analytical models for assessing security against unauthorized access and maintaining the confidentiality of information are considered. Based on the methods of recovery theory and approximation of the distribution functions used by two-parameter distributions, a mathematical apparatus has been developed for assessing the security of information from unauthorized access. The proposed theoretical provisions for security assessment extend the well-known standardized calculation methods using one-parameter approximation of distribution functions, are quite universal and can be useful to a wide range of specialists.

Keywords: models, standard, recommendations, confidentiality, information protection, recovery processes, distribution function, approximation, unauthorized access.

Введение

В национальном стандарте Российской Федерации ГОСТ Р 59341-202 «Системная инженерия. Защита информации в процессе управления информацией системы» определены типовые методы, модели и методические указания по прогнозированию рисков, типовые допустимые значения для расчетных показателей и примерный перечень методик системного анализа. В соответствии с рекомендацией В.3.9.3 данного стандарта рассмотрена модель для оценки защищенности от несанкционированного доступа (НСД), а в соответствии с рекомендацией В.3.9.4 представлена модель для оценки сохранения конфиденциальности используемой информации. В данных моделях при аппроксимации функций распределения (ФР) времени выполнения исследуемых процессов экспоненциальным распределением получены простые расчетные формулы для оценки вероятностных показателей защищенности информации от НСД. Представляет несомненный практический интерес учет не только средних значений ФР временных параметров исследуемых процессов, но их дисперсии и разработки аналитических моделей оценки защищенности от НСД, учитывающих два первых момента реальных ФР и аппроксимации их эквивалентными ФР в смысле равенства математических ожиданий и дисперсий. Именно этой проблематике и посвящена настоящая статья. Рассмотренный ниже подход может быть использован в дальнейшем для расширения рекомендаций В.3.9.3 и В.3.9.4.

Для исследования эффективности систем защиты базовых информационных технологий от НСД предлагается использовать системный подход, базирующийся на теории случайных процессов, расширяющий область применения моделей, описанных в рекомендациях В.3.9.3, В.3.9.4 и в работе [1], на основе методов теории восстановления и аппроксимации используемых функций распределения двухпараметрическими распределениями Эрланга и гиперэкспоненциальными двухпараметрическими распределениями [2].

Информационные и программные ресурсы i-го типа считаются достаточно защищенными от несанкционированного доступа (НСД), если с учетом возможности потенциального преодоления преград вероятность сохранения защищенности системы $\mathrm{P}_{\text{защ}(i)} \geq \mathrm{P}_{\text{доп}(i)}$, где $P_{доп(i)}$ - задаваемая допустимая вероятность сохранения защищенности ресурсов i-го типа.

Формализация процессов несанкционированного доступа к ресурсам рассмотрена в работе [1].

Вероятность предотвращения НСД:

$\mathrm{P}_{\text{защ}(i)} = 1 - \prod_{m=1}^{\kappa} P_{НСД\ (m)}$, (1)

где κ количеству преград, которые необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам i-го типа;

$\mathrm{P}_{\text{НСД}(m)}$- вероятность преодоления нарушителем m -ой преграды.

Модель базируется на использовании методов теории восстановления, с помощью которых оценивается вероятность преодоления нарушителем каждой из преград системы защиты.

В модели не учитывается функция распределения периода объективной конфиденциальности $B_{конф\ (i)}(t)$.

В остальном модель соответствует модели сохранения конфиденциальности.

Для оценки $P_{НСД(m)}$ необходимо задать:

$F_{mi}(t)$ - ФР времени между соседними изменениями параметров m -ой преграды системы защиты ресурсов i-го типа $(m = \overline{1,\kappa})$;

$U_{mi}(t)$ - ФР времени расшифровки значений параметров m -ой преграды системы ресурсов i-го типа $(m = \overline{1,\kappa})$.

Оценка параметров ФР $F_{mi}(t)$ и $U_{mi}(t)$ может потребовать на практике использования дополнительных моделей.

Пусть $\{t_n\}_{n=1}^{\infty}$ процесс восстановления. Моменты t_n соответствуют времени изменения параметров m -ой преграды системы защиты ресурсов i-го типа.

Последовательности точек регенерации $\{t_n\}$поставим в соответствие случайную функцию

$\xi_m(t) = U_{mi}(t - t_n)$ при $t_n \leq t < t_{n+1}$, $n \geq 1$

$\xi_m(t) = 0$ при $0 \leq t < t_1$

$\xi_m(t)$ в интервале$t_n \leq t < t_{n+1}$, $(n \geq 1)$ является вероятностью того, что нарушитель ко времени t расшифровал значения параметров m -ой защиты ресурсов i-го типа

В соответствии со свойством 1 для процессов восстановления [3]:

$P_{НСД\ (m)} = M\xi_m(t) = \int_0^t \{[1 - F_{m\ i}(t - x)] U_{m\ i}(t - x)\} dH_m(x)$, (2)

где $H_m(t)$ - функция восстановления.

В соответствии с предельной теоремой теории восстановления [3]:

$P_{НСД\ (m)} = \frac{1}{F_{mi}^{(1)}} \int_0^{\infty} [1 - F_{mi}(t)]\, U_{mi}(t) dt$, (3)

где $F_{mi}^{(1)}$ 1-ый момент ФР $F_{mi}(t)$

На 1-ом этапе при реализации стандартных методов расчета ФР $F_{mi}(t)$ и $U_{mi}(t)$ выбираются из класса экспоненциальных или детерминированных функций. Поэтому для определения ФР $F_{mi}(t)$ и $U_{mi}(t)$ достаточно задать только математические ожидания этих ФР.

В настоящей работе ФР $F_{mi}(t)$ и $U_{mi}(t)$ выбираются из класса двухпараметрических гиперэкспоненциальных и эрланговских ФР.

Рассмотрим модель оценки конфиденциальности информации при ограничении на время защиты

Определение. Информация i-го типа, представляемая пользователю из БД, считается конфиденциальной, если на момент использования этой информации несанкционированный доступ к информационным ресурсам i-го типа не состоялся до истечения периода объективной конфиденциальности с вероятностью

$P_{конф(i)} \geq P_{доп(i)}$, где $P_{доп(i)}$ - задаваемая допустимая вероятность сохранения конфиденциальности информации i-го типа.

Для доступа к хранимым в системе ресурсам выстраивается последовательность преград от злоумышленника с тем, чтобы допущенный пользователь, зная и реализуя алгоритм преодоления этих преград, мог решить свои задачи в установленном штатном режиме. В качестве нарушителя рассматривается лицо, не посвященное в тайну преодоления защитных преград. Вскрывая каким-либо доступным образом алгоритм преодоления преград, злоумышленник вполне может получить доступ к ресурсам системы.

Нарушитель в состоянии проникнуть в систему лишь при условиях:

во-первых, ему станет известна система защиты в части, необходимой для достижения его целей;

во-вторых, он успеет получить доступ к информационным или программным ресурсам до того, как система защиты видоизменится (после чего перед нарушителем возникнет проблема повторного преодоления защитных преград).

Для оценки $P_{конф(i)}$ используется метод расчета вероятностей преодоления нарушителем каждой из преград системы защиты, базирующейся на методах теории восстановления.

Проведем оценку вероятности сохранения конфиденциальности информации i-го типа для систем, использующих $к$ преград, которые необходимо преодолеть нарушителю, чтобы получить доступ к информации i-го типа с использованием методов теории случайных процессов восстановления.

Вероятность сохранения конфиденциальности [1]:

$$\mathrm{P}_{\text{конф}(i)} = 1 - \prod_{m=1}^{к} P_{НСД\ \ конф(m)}, \qquad (4)$$

где к - количество преград, которые необходимо преодолеть нарушителю, чтобы получить доступ к информации i-го типа;

$\mathrm{P}_{\text{НСД конф }(m)}$ - вероятность преодоления нарушителем m -ой преграды системы защиты информации i-го типа;

Для оценки $\mathrm{P}_{\text{НСД конф }(m)}$ необходимо задать:

$U_{mi}(t)$ - ФР времени расшифровки значений параметров m -ой преграды системы защиты информации i-го типа $(m = \overline{1, к})$;

$F_{mi}(t)$ - ФР времени между соседними изменениями параметров m -ой преграды системы защиты ресурсов i-го типа $(m = \overline{1, к})$;

$B_{конф\ \ (i)}(t)$ - ФР периода объективной конфиденциальности информации i-го типа;

Для оценки параметров ФР $U_{mi}(t)$, $F_{mi}(t)$, $B_{конф\ \ (i)}(t)$ на практике могут потребоваться дополнительные модели.

Пусть $\{t_n\}_{n=1}^{\infty}$ процесс восстановления, моменты t_n которого соответствуют времени изменения параметров m -ой преграды системы защиты информации i-го типа.

Будем считать, что $\mathrm{B}_{\text{конф }(i)}$ является экспоненциальной функцией. При этом имеет место отсутствие последствия для этой ФР. Предположим также, что $\mathrm{B}^{(1)}_{\text{конф}\ \ i} >> F^{(1)}_{m\ \ i}$ и $U^{(1)}_{m_i} >> F^{(1)}_{m\ \ i}$

Последовательность точек регенерации $\{t_n\}$ поставим в соответствие случайную функцию $\xi(t)$, при построении которой используется дифференциальный подход:

$$\xi_m(t) = \int_0^{t-t_n} dU_{mi}(\theta)(1 - B_{\text{конф}(i)}(\theta)), \quad \text{при } t_n \le t < t_{n+1} \ \ n \ge 1$$

$$\xi_m(t) = 0 \qquad 0 \le t < t_1$$

В соответствии со свойством 1 для процессов восстановления [3]:

$$P_{НСД\ \ конф(m)} = M\xi_m(t) = \int_0^t \left\{[1 - F_{mi}(t - x)] \int_0^{t-x} (1 - B_{конф(i)}(\theta)) dU_{mi}(\theta)\right\} dH(x), \qquad (5)$$

и в соответствии с предельной теоремой теории восстановления [3]:

$$P_{НСД\ \ конф(m)} = \frac{1}{F^{(1)}_{mi}} \int_0^{\infty} \left\{[1 - F_{mi}(t)] \int_0^t \left[dU_{mi}(\theta) \cdot (1 - B_{конф(i)}(\theta))\right]\right\} dt. \qquad (6)$$

При разработке программных продуктов, предназначенных для оценки $\mathrm{P}_{\text{конф}(i)}$ (формулы (4) ÷ (6)), в стандартизованных методах расчета выбирают ФР $F_{mi}(t)$, $U_{mi}(t)$ из класса экспоненциальных и детерминированных.

Не представляет трудностей получение расчетных формул для этого случая. Именно эти формулы и являются основой для стандартизации методов расчета защищенности информации в многоуровневых системах защиты.

Рассмотрим аналитический подход, расширяющий область применимости стандартизованных методов расчета.

Математический аппарат, использующий двухпараметрическую аппроксимацию ФР при оценке защищенности от НСД и сохранении конфиденциальности информации

Пусть известны 2-а момента некоторых непрерывных функций распределения (ФР). Две ФР считаются эквивалентными, если равны их первые и вторые моменты.

Множество используемых при дальнейшем рассмотрении аппроксимирующих эквивалентных ФР будем выбирать из класса двухпараметрических функций: при коэффициенте вариации большем 1 – это гиперэкспоненциальные двухпараметрические ФР специального вида, при коэффициенте вариации меньшем 1 – это распределения Эрланга k-го порядка.

Распределение Эрланга является последовательной суперпозицией экспоненциальных ФР, а гиперэкспоненциальное распределение является параллельной суперпозицией экспоненциальных ФР. Это позволяет непосредственно без численного интегрирования получить аналитические выражения для интегральных соотношений (3) и (6). Практически по экспериментальным данным с приемлемой точностью можно определить только 1-ый и 2-ой моменты ФР и легко определяемую по ним дисперсию. Поэтому аппроксимацию ФР по 1-му моменту и дисперсии целесообразно проводить в зависимости от коэффициента вариации либо распределением Эрланга, либо гиперэкспоненциальным распределением, имеющим значение 1-го момента и дисперсии, совпадающие с экспериментально определенными 1-ым моментом и дисперсией. При этом удается непосредственно получить расчетные соотношения для оценки вероятности несанкционированного доступа, не прибегая к численному интегрированию соотношений (3) и (6). Отметим, что именно Эрланговская и гиперэкспоненциальная аппроксимации позволяют расширить методы элементарной теории массового обслуживания с экспоненциальными ФР на использование аналитических методов исследования систем массового обслуживания общего вида.

Если известны два момента ФР $B_i(t)$: $B_i^{(1)}$и $B_i^{(2)}$, то коэффициент вариации C_i равен:

$$C_i = \sqrt{(B_i^{(2)} - (B_i^{(1)})^2)/(B_i^{(1)})^2}$$

В том случае, если $C_i \geq 1$ в качестве аппроксимирующих эквивалентных ФР выбирается двухпараметрическое гиперэкспоненциальное распределение

$$B_{АП(i)}(t) = 1 - \phi e^{-2\phi\lambda t} - (1-\phi)e^{-2(1-\phi)\lambda t} \quad , \qquad (7)$$

где $\lambda = \frac{1}{B_i^{(1)}}$; $\phi = \frac{1}{2} - \sqrt{\frac{1}{4} - \frac{1}{2(1+C^2)}}$, $0 < \phi \leq \frac{1}{2}$.

При $C_i = 1$ двухпараметрическое гиперэкспоненнциальное распределение вырождается в однопараметрическое экспоненциальное и аппроксимирующими становятся экспоненциальные ФР

$B_{АП(i)}(t) = 1 - e^{-\lambda t}$, где $\lambda = \frac{1}{B_i^{(1)}}$, и в этом случае мы получим известные стандартизованные формулы для расчета.

При $C_i < 1$ в качестве аппроксимирующих ФР выбираются распределения Эрланга k-го порядка:

$$A_{АП(i)}(t) = 1 - e^{-\lambda kt}\sum_{n=0}^{k-1}\frac{(\lambda kt)^n}{n!} , \qquad (8)$$

где $k = ent[\frac{1}{C_i^2} + 0.5]$, $C_i^2 = \frac{A_i^{(2)} - (A_i^{(1)})^2}{(A_i^{(1)})^2}$, $\lambda = \frac{1}{A_i^{(1)}}$.

При k=2 $A_{АП(i)}(t) = 1 - e^{-\lambda 2t}(1 + \lambda 2t)$

При k=3 $A_{АП(i)}(t) = 1 - e^{-\lambda 3t}(1 + \lambda 3t + \frac{(\lambda 3t)^2}{2})$.

Несанкционированный доступ к ресурсам i-го типа при коэффициенте вариации ФР $U_{(i)m}(t)$ преодоления m-ой преграды $C_i > 1$

Как отмечено выше, вероятность предотвращения НСД к ресурсам i-го типа:

$P_{защ(i)} = 1 - \prod_{m=1}^{k} P_{НСД_{(i)m}}$,

где k— количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам i-го типа;

$P_{НСД_{(i)m}}$— вероятность преодоления нарушителем m-й преграды:

$$P_{НСД_{(i)m}} = \frac{1}{f_{(i)m}}\int_0^\infty [1 - F_{(i)m}(t)]U_{(i)m}(t)\mathrm{dt}$$

где $F_{(i)m}(t)$ - ФР времени между соседними регламентирующими изменениями параметров m-й преграды системы защиты ресурсов i-го типа (приводящих к необходимости новой их расшифровки нарушителем);

$U_{(i)m}(t)$ - ФР времени расшифровки значений параметров m-й преграды системы защиты ресурсов i-го типа.

Экспоненциальное приближение ФР $F_{(i)m}(t)$ и гиперэкспоненциальное приближение ФР $U_{(i)m}(t)$:

$U_{(i)m}(t) = 1 - \phi\, exp(-2\phi\lambda_{im}t) - (1-\phi)\, exp(-2(1-\phi)\lambda_{im}t)$,

$\lambda_{im} = \frac{1}{u_{(i)m}}$, $u_{(i)m} = \int_0^\infty t dU_{(i)m}(t)$

$F_{(i)m}(t) = 1 - exp(-t * f_{(i)m}^{-1})$, $f_{(i)m} = \int_0^\infty t dF_{(i)m}(t)$

Следовательно $1 - F_{(i)m}(t) = exp(-t * f_{(i)m}^{-1})$, тогда

$$P_{НСД_{(i)m}} = \frac{1}{f_{(i)m}}\int_0^\infty [1 - F_{(i)m}(t)]U_{(i)m}(t)\mathrm{dt} =$$

$$= \frac{1}{f_{(i)m}}\int_0^\infty exp(-t/f_{(i)m})[1 - \phi\, exp(-2\phi\lambda_{im}t) - (1-\phi)\, exp(-2(1-\phi)\lambda_{im}t)]dt =$$

$$= 1 - \frac{\phi \frac{1}{f_{(i)m}}}{\frac{1}{f_{(i)m}} + 2\phi\lambda_{im}} - \frac{(1-\phi)\frac{1}{f_{(i)m}}}{\frac{1}{f_{(i)m}} + 2(1-\phi)\lambda_{im}} \qquad (9)$$

При $\phi = \frac{1}{2}$ двухпараметрическое гиперэкспоненциальное распределение переходит в экспоненциальное, и мы имеем известную формулу:

$$P_{\text{НСД}_{(i)m}} = \frac{\frac{1}{u_{(i)m}}}{\frac{1}{f_{(i)m}} + \frac{1}{u_{(i)m}}} \qquad (10)$$

Учитывая формулу (1), получим следующее выражение для $P_{\text{защ}_{(i)m}}$:

$$P_{защ(i)m} = \frac{\phi \frac{1}{f_{(i)m}}}{\frac{1}{f_{(i)m}} + 2\phi\lambda_{im}} + \frac{(1-\phi)\frac{1}{f_{(i)m}}}{\frac{1}{f_{(i)m}} + 2(1-\phi)\lambda_{im}} \qquad (11)$$

Гиперэкспоненциальное приближение $C_i > 1$ФР $U_{(i)m}(t)$ и детерминированное приближение ФР $F_{(i)m}(t)$:

$U_{(i)m}(t) = 1 - \phi\, exp(-2\phi\lambda_{im}t) - (1-\phi)\, exp(-2(1-\phi)\lambda_{im}t),$

$\lambda_{im} = \frac{1}{u_{(i)m}}$, $u_{(i)m} = \int_0^\infty t dU_{(i)m}(t)$

$F_{(i)m}(t) = \begin{cases} 0, \text{при } t \le f_{(i)m} \\ 1, \text{при } t > f_{(i)m} \end{cases}, \qquad f_{(i)m} = \int_0^\infty t dF_{(i)m}(t)$

Следовательно, $1 - F_{(i)m}(t) = \begin{cases} 1, при\ t \le f_{(i)m} \\ 0, при\ t > f_{(i)m} \end{cases}$, тогда:

$$P_{\text{НСД}_{(i)m}} = \frac{1}{f_{(i)m}} \int_0^\infty [1 - F_{(i)m}(t)] U_{(i)m}(t) \mathrm{dt} = \frac{1}{f_{(i)m}} \int_0^{f_{(i)m}} U_{(i)m}(t) dt =$$

$$= \frac{1}{f_{(i)m}} \int_0^{f_{(i)m}} [1 - \phi\, exp(-2\phi\lambda_{im}t) - (1-\phi)\, exp(-2(1-\phi)\lambda_{im}t)] dt =$$

$$= 1 - \frac{1}{2\lambda_{im} f_{(i)m}} (1 - exp(-2\phi\lambda_{im} f_{(i)m})) - \frac{1}{2\lambda_{im} f_{(i)m}} (1 - exp(-2(1-\phi)\lambda_{im} f_{(i)m})) \qquad (12)$$

$$P_{\text{защ}(i)m} = 1 - \mathrm{P}_{\text{НСД}_{(i)m}} = \frac{u_{(i)m}}{2f_{(i)m}} [1 - e^{-2\phi \frac{f_{(i)m}}{u_{(i)m}}}] + \frac{u_{(i)m}}{2f_{(i)m}} [1 - e^{-2(1-\phi)\frac{f_{(i)m}}{u_{(i)m}}}] \ (13)$$

Экспоненциальное приближение ФР $F_{(i)m}(t)$ и к-распределение Эрланга ($C_i < 1$) для приближения ФР $U_{(i)m}(t)$:

$U_{(i)m}(t) = 1 - e^{-\lambda kt} \sum_{n=0}^{k-1} \frac{(\lambda kt)^n}{n!}$,

где $k = ent[\frac{1}{C_i^2} + 0.5]$, $C_i^2 = \frac{U_{(i)m}^{(2)} - (U_{(i)m}^{(1)})^2}{(U_{(i)m}^{(1)})^2}$, $\lambda = \frac{1}{u_{(i)m}}$,

$u_{(i)m} = \int_0^\infty t dU_{(i)m}(t)$, $\qquad u_{(i)m} = U_{(i)m}^{(1)}$,

$F_{(i)m}(t) = 1 - exp(-t * f_{(i)m}^{-1}),$ $\qquad f_{(i)m} = \int_0^\infty t dF_{(i)m}(t)$

Следовательно, $1 - F_{(i)m}(t) = exp(-t * f_{(i)m}^{-1})$, тогда

$$P_{\text{НСД}_{(i)m}} = \frac{1}{f_{(i)m}} \int_0^\infty [1 - F_{(i)m}(t)] U_{(i)m}(t) \mathrm{dt} =$$

$$= \frac{1}{f_{(i)m}} \int_0^\infty \exp(-t/f_{(i)m}) \{1 - e^{-\lambda kt} \sum_{n=0}^{k-1} \frac{(\lambda kt)^n}{n!}\} \mathrm{dt} = \frac{(k\lambda)^k}{(\frac{1}{f_{(i)m}} + k\lambda)^k} = \frac{(k\frac{1}{u_{(i)m}})^k}{(\frac{1}{f_{(i)m}} + k\frac{1}{u_{(i)m}})^k} \ (14)$$

$$P_{\text{защ(i)m}} = 1 - P_{\text{НСД}_{(i)m}} = 1 - \frac{(k\frac{1}{u_{(i)m}})^k}{(\frac{1}{f_{(i)m}} + k\frac{1}{u_{(i)m}})^k} \qquad (15)$$

Несанкционированный доступ к ресурсам i-го типа в течение заданного директивного периода (конфиденциальность)

Выше отмечено, что вероятность предотвращения НСД к ресурсам i-го типа в течение заданного периода времени $P_{конф(i)}$ равна:

$P_{конф(i)} = 1 - \prod_{m=1}^{k} P_{НСД\ \ конф(i)m}$,

где k – количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к ресурсам i-го типа в течение заданного директивного времени;

$P_{НСД\cdot конф(i)m}$ – вероятность преодоления нарушителем m-й преграды за время, не превышающее директивное (директивное время - период объективной конфиденциальности):

$$P_{НСД\ \ конф(i)m)} = \frac{1}{f_{(i)m}} \int_0^{\infty} \left\{ \left[1 - F_{(i)m}(t)\right] \int_0^t \left[dU_{(i)m}(\theta) \cdot (1 - B_{конф(i)}(\theta))\right] \right\} dt$$

где $F_{(i)m}(t)$ - ФР времени между соседними регламентирующими изменениями параметров m-й преграды системы защиты ресурсов i-го типа (приводящих к необходимости новой их расшифровки нарушителем);

$U_{(i)m}(t)$ - ФР времени расшифровки значений параметров m-й преграды системы защиты ресурсов i-го типа за время, не превышающее директивное.

$B_{конф\ \ (i)}(t)$ - ФР периода объективной конфиденциальности информации i-го типа.

Экспоненциальное приближение ФР $F_{(i)m}(t)$, $B_{конф\ \ (i)}(t)$ и гиперэкспоненциальное приближение ФР $U_{(i)m}(t)$:

$U_{(i)m}(t) = 1 - \phi\, exp(-2\phi\lambda_{im}t) - (1-\phi)\, exp(-2(1-\phi)\lambda_{im}t)$,

$\lambda_{im} = \frac{1}{u_{(i)m}}$, $u_{(i)m} = \int_0^{\infty} t dU_{(i)m}(t)$

$F_{(i)m}(t) = 1 - exp(-t * f_{(i)m}^{-1})$, $\quad f_{(i)m} = \int_0^{\infty} t dF_{(i)m}(t)$

$B_{конф(i)}(t) = 1 - exp(-t * h_{(i)}^{-1})$, $\quad h_{(i)} = \int_0^{\infty} t dB_{конф(i)}(t)$

Следовательно, $1 - F_{(i)m}(t) = exp(-t * f_{(i)m}^{-1})$,

$dU_{(i)m}(\theta) = \{2\phi^2\lambda_{(i)m}\, exp(-2\phi\lambda_{(i)m}\theta) + 2(1-\phi)^2\lambda_{(i)m}\, exp(-2(1-\phi)\lambda_{(i)m}\theta)\}d\theta$, тогда

$$\int_0^t \left[1 - B_{\text{конф}(i)}(\theta)\right] \mathrm{dU}_{(i)m}(\theta) = \int_0^t e^{-\theta/h_{(i)}} \{2\phi^2\lambda_{(i)m} e^{-2\phi\lambda_{(i)m}\theta} + 2(1-\phi)^2\lambda_{(i)m} e^{-2(1-\phi)\lambda_{(i)m}\theta}\} d\theta =$$
$$= \frac{2\phi^2\lambda_{(i)m}}{2\phi\lambda_{(i)m} + \frac{1}{h_{(i)}}} - \frac{2\phi^2\lambda_{(i)m}}{2\phi^2\lambda_{(i)m} + \frac{1}{h_{(i)}}} exp(-t(2\phi\lambda_{(i)m} + \frac{1}{h_{(i)}})) + \frac{2(1-\phi)^2\lambda_{(i)m}}{2(1-\phi)\lambda_{(i)m} + \frac{1}{h_{(i)}}} -$$
$$- \frac{2(1-\phi)^2\lambda_{(i)m}}{2(1-\phi)\lambda_{(i)m} + \frac{1}{h_{(i)}}} exp(-t(2(1-\phi)\lambda_{(i)m} + \frac{1}{h_{(i)}}))$$

$$\int_0^{\infty} \{[1 - F_{(i)m}(t)] \int_0^t \left[1 - B_{\text{конф}(i)}(\theta)\right] \mathrm{dU}_{(i)m}(\theta)\} \mathrm{dt} = \int_0^{\infty} \{e^{-t/f_{(i)m}} \int_0^t [1 - B_{конф(i)}] dU_{(i)m}\} dt =$$

$$= f_{(i)m} \frac{2\phi^2\lambda_{(i)m}}{2\phi\lambda_{(i)m} + \frac{1}{h_{(i)}}} (1 - \frac{\frac{1}{f_{(i)m}}}{2\phi\lambda_{(i)m} + \frac{1}{h_{(i)}} + \frac{1}{f_{(i)m}}}) + f_{(i)m} \frac{2(1-\phi)^2\lambda_{(i)m}}{2(1-\phi)\lambda_{(i)m} + \frac{1}{h_{(i)}}} (1 - \frac{\frac{1}{f_{(i)m}}}{2(1-\phi)\lambda_{(i)m} + \frac{1}{h_{(i)}} + \frac{1}{f_{(i)m}}})$$

$$P_{НСДконф(i)m} = \frac{2\phi^2\lambda_{(i)m}}{2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}}}\left(1-\frac{\frac{1}{f_{(i)m}}}{2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}}+\frac{1}{f_{(i)m}}}\right)+\frac{2(1-\phi)^2\lambda_{(i)m}}{2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}}}\left(1-\frac{\frac{1}{f_{(i)m}}}{2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}}+\frac{1}{f_{(i)m}}}\right)=$$

$$=\frac{2\phi^2\lambda_{(i)m}}{2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}}+\frac{1}{f_{(i)m}}}+\frac{2(1-\phi)^2\lambda_{(i)m}}{2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}}+\frac{1}{f_{(i)m}}} \qquad (16)$$

$$P_{защ.конф(i)m} = 1-P_{НСДконф(i)m} = 1-\left\{\frac{2\phi^2\lambda_{(i)m}}{2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}}+\frac{1}{f_{(i)m}}}+\frac{2(1-\phi)^2\lambda_{(i)m}}{2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}}+\frac{1}{f_{(i)m}}}\right\} \qquad (17)$$

Экспоненциальное приближение ФР $B_{конф\ (i)}(t)$, гиперэкспоненциальное приближение ФР $\boldsymbol{U_{(i)m}(t)}$ и детерминированное приближение ФР $\boldsymbol{F_{(i)m}(t)}$:

$$U_{(i)m}(t) = 1-\phi\, exp(-2\phi\lambda_{im}t)-(1-\phi)\, exp(-2(1-\phi)\lambda_{im}t),$$

$$\lambda_{im} = \frac{1}{u_{(i)m}}\ , u_{(i)m} = \int_0^\infty t dU_{(i)m}(t)$$

$$\phi = \frac{1}{2}-\sqrt{\frac{1}{4}-\frac{1}{2(1+C^2)}},\quad 0<\phi\le\frac{1}{2}\ ,$$

$$C^2 = \frac{[\int_0^\infty t^2 dU_{(i)m}(t)]-[\int_0^\infty t dU_{(i)m}(t)]^2}{[\int_0^\infty t dU_{(i)m}(t)]^2}\ ;$$

$$B_{конф(i)}(t) = 1-exp(-t*h_{(i)}^{-1}),\quad h_{(i)} = \int_0^\infty t dB_{конф(i)}(t)$$

$$F_{(i)m}(t) = \begin{cases}0, при\ t\le f_{(i)m}\\ 1, при\ t> f_{(i)m}\end{cases},\qquad f_{(i)m} = \int_0^\infty t dF_{(i)m}(t)$$

В этом случае получим:

$$\int_0^t\left[1-B_{конф(i)}(\theta)\right]dU_{(i)m}(\theta) = \int_0^t e^{-\theta/h_{(i)}}\{2\phi^2\lambda_{(i)m}e^{-2\phi^2\lambda_{(i)m}\theta}+2(1-\phi)^2\lambda_{(i)m}e^{-2(1-\phi)\lambda_{(i)m}\theta}\}d\theta =$$
$$=\frac{2\phi^2\lambda_{(i)m}}{2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}}}-\frac{2\phi^2\lambda_{(i)m}}{2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}}}exp(-t(2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}}))+\frac{2(1-\phi)^2\lambda_{(i)m}}{2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}}}-$$
$$-\frac{2(1-\phi)^2\lambda_{(i)m}}{2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}}}exp(-t(2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}}))$$

$$\int_0^\infty\{[1-F_{(i)m}(t)]\int_0^t\left[1-B_{конф(i)}(\theta)\right]dU_{(i)m}(\theta)\}dt = \left(\frac{2\phi^2\lambda_{(i)m}}{2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}}}+\frac{2(1-\phi)^2\lambda_{(i)m}}{2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}}}\right)\int_0^{f_{(i)m}}dt-$$
$$-\frac{2\phi^2\lambda_{(i)m}}{2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}}}\int_0^{f_{(i)m}}e^{-t(2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}})}dt-\frac{2(1-\phi)^2\lambda_{(i)m}}{2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}}}\int_0^{f_{(i)m}}e^{-t(2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}})}dt =$$
$$= f_{(i)m}\left(\frac{2\phi^2\lambda_{(i)m}}{2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}}}+\frac{2(1-\phi)^2\lambda_{(i)m}}{2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}}}\right)+\frac{2\phi^2\lambda_{(i)m}}{(2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}})^2}exp[-f_{(i)m}(2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}})]-$$
$$-\frac{2\phi^2\lambda_{(i)m}}{(2\phi\lambda_{(i)m}+\frac{1}{h_{(i)}})^2}+\frac{2(1-\phi)^2\lambda_{(i)m}}{(2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}})^2}exp[-f_{(i)m}(2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}})]-\frac{2(1-\phi)^2\lambda_{(i)m}}{(2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}})^2}$$

$$P_{НСДконф(i)m} = \frac{2\phi^2\lambda_{(i)m}}{2\phi\lambda_{(i)m} + \frac{1}{h_{(i)}}} + \frac{2(1-\phi)^2\lambda_{(i)m}}{2(1-\phi)\lambda_{(i)m} + \frac{1}{h_{(i)}}} + \frac{2\phi^2\lambda_{(i)m}\frac{1}{f_{(i)m}}}{(2\phi\lambda_{(i)m} + \frac{1}{h_{(i)}})^2}\{exp[-f_{(i)m}(2\phi\lambda_{(i)m} + \frac{1}{h_{(i)}})] - 1\} +$$

$$+\frac{2(1-\phi)^2\lambda_{(i)m}\frac{1}{f_{(i)m}}}{(2(1-\phi)\lambda_{(i)m}+\frac{1}{h_{(i)}})^2}\{exp[-f_{(i)m}(2(1-\phi)\lambda_{(i)m} + \frac{1}{h_{(i)}})] - 1\} \quad (18)$$

$$P_{ЗАЩконф(i)m} = 1 - P_{НСДконф(i)m} \quad (19)$$

Таким образом, формулы (9), (10), (11), (12), (13), (14), (15) позволяют рассчитать защищенность i-ых ресурсов системы m-ой преградой от НСД, а формулы (16), (17), (18), (19) – защищенность i-ых ресурсов m-ой преградой от НСД в течение заданного периода объективной конфиденциальности информации i-го типа при различных политиках смены параметров этой преграды.

Заключение

В работе изложены теоретические положения по оценке защищенности от НСД и сохранения конфиденциальности используемой информации, позволяющие получить аналитические соотношения для расчета защищенности информации по экспериментально определенным 1-му моменту и дисперсии ФР времени преодоления нарушителем преграды и по первым двум моментам ФР интервала смены параметров преграды. На основе методов теории восстановления и двухпараметрической аппроксимации используемых функций распределения разработан математический аппарат для оценки защищенности информационных технологий от НСД, расширяющий область применимости моделей, описанных в рекомендациях B.3.9.3 и B.3.9.4 ГОСТ Р 59341-202 «Системная инженерия. Защита информации в процессе управления информацией системы». Полученные формулы для расчета защищенности информации от НСД нашли практическое применение при разработке комплекса программ оценки защищенности от НСД, расширяющего область применимости программ, реализующих стандартизованные методы расчета.

Список литературы

1. Бескоровайный М.М., Костогрызов А. И., Львов В. М. Инструментально-моделирующий комплекс для оценки качества функционирования информационных систем «КОК»: Руководство системного аналитика. - М.: Вооружение. Политика. Конверсия. - 2002. – 305с.
2. Колесников Г. С., Леонтьев А. С., Ткаченко В. М. «Аналитические методы оценки защищенности информационных технологий при разработке многоуровневых систем защиты»: Учебное пособие // Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский государственный технический университет радиотехники, электроники и автоматики» - М.: МИРЭА, 2013. – 60с.
3. Гнеденко Б. В., Коваленко И. Н. Введение в теорию массового обслуживания. М.: Наука. Гл. ред. физ.-мат. лит. – 1987.-336с.

References

1. Beskorovainy M.M., Kostogryzov A.I., Lvov V.M. Instrumental-modeling complex for assessing the quality of functioning of information systems "KOC": A guide for a system analyst. - M.: Armament. Politics. Conversion. - 2002. - 305s.
2. Kolesnikov G. S., Leontiev A. S., Tkachenko V. M. “Analytical methods for assessing the security of information technologies in the development of multi-level protection systems”: Textbook // Federal State Budgetary Educational Institution of Higher Professional Education “Moscow State Technical University radio engineering, electronics and automation" - M.: MIREA, 2013. - 60p.
3. Gnedenko B. V., Kovalenko I. N. Introduction to the theory of queuing. M.: Science. Ch. ed. Phys.-Math. lit. – 1987.-336s.