DOI 10.46566/2500-4050_2023_77_126
УДК 004.056.53

Леонтьев А.С., к.т.н.
старший научный сотрудник
доцент
кафедра МОСИТ
МИРЭА – Российский технологический университет
Россия, г.Москва
ORCID: 0000-0003-3673-2468
Тимошкин М.С.
студент магистратуры
МИРЭА – Российский технологический университет
Россия, г.Москва
ORCID: 0000-0003-1842-8331

АСИМПТОТИЧЕСКИЕ МЕТОДЫ ОЦЕНКИ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ С МНОГОУРОВНЕВЫМИ СИСТЕМАМИ ЗАЩИТЫ

Аннотация: рассмотрены вопросы использования аналитических моделей для оценки защищенности информационных технологий от несанкционированного доступа и сохранения конфиденциальности информации. На основе методов теории восстановления и аппроксимации используемых функций однопараметрическими распределениями разработан математический аппарат асимптотической теории для оценки защищенности информационных технологий с многоуровневыми системами защиты, позволяющий оперативно исследовать эффективность различных рубежей защиты и выбирать многоуровневые системы защиты, удовлетворяющие требованиям заказчика. Полученные аналитические соотношения нашли практическое применение при оперативной оценке вероятностных показателей защищенности информации от несанкционированного доступа в вычислительных системах различного назначения.

Ключевые слова: теория восстановления, защищенность информации, аппроксимация, асимптотические методы, многоуровневые системы защиты, рубежи защиты, несанкционированный доступ.

Leontyev A.S., Ph.D. of engineering sciences
senior research officer
associate professor
Department of Mathematical Support and Standardization of Information Technologies
MIREA – Russian Technological University

Russian Federation, Moscow
ORCID: 0000-0003-3673-2468
Timoshkin M.S.
master student
MIREA – Russian Technological University
Russian Federation, Moscow
ORCID: 0000-0003-1842-8331

ASYMPTOTIC METHODS FOR ASSESSING INFORMATION SECURITY INDICATORS IN COMPUTING SYSTEMS WITH MULTILEVEL PROTECTION SYSTEMS

Abstract: the issues of using analytical models for assessing the security of information technologies from unauthorized access and maintaining the confidentiality of information were considered. Based on the methods of recovery theory and approximation of the functions used by one-parameter distributions, a mathematical apparatus of asymptotic theory has been developed for assessing the security of information technologies with multi-level protection systems, which allows quickly investigate the effectiveness of various protection frontiers and select multi-level protection systems that meet customer requirements. The obtained analytical relationships have found practical application in the operational assessment of probabilistic indicators of information security from unauthorized access in computing systems for various purposes.

Keywords: recovery theory, information security, approximation, asymptotic methods, multilevel security systems, security frontiers, unauthorized access.

Введение.

Современные информационные системы (ИС) – это системы, выполняющие свои функции посредством технологических операций сбора, хранения, обработки и представления информации на основе интеграции возможностей человека, компьютеров, программных средств и средств связи. Требования к функционированию ИС формируются с учетом целей системы в целом, условий использования ИС (в т.ч. потенциальных угроз), выделяемых ресурсов на создание и эксплуатацию, функциональных возможностей источников информации, требований со стороны управляемых объектов, а также требований и условий взаимодействия с другими системами. При этом особое внимание отводится безопасности информации и безопасности деятельности человека [1, 2, 3, 4, 5].

На практике выходная информация является результатом многогранной переработки входной информации от различных

источников. Кроме того, интегральное качество используемой информации существенным образом зависит от типов решаемых функциональных задач, их защищенности, содержания и достоверности получаемой в результате решения выходной информации и от требований пользователей в конкретных условиях функционирования системы. Эти зависимости должны учитываться при детальной оценке безопасности сложных систем [6, 7, 8].

Зачастую для того, чтобы выявить нужные количественные закономерности в процессах (технологических операциях) сбора, хранения, обработки и представления информации, при построении моделей оценки защищенности информационных технологий и оценке эффективности систем защиты оказывается необходимым пренебречь деталями обработки и проанализировать отдельные смысловые элементы информации и их защищенность с момента их появления до использования [9, 10, 11, 12].

В настоящей работе предлагается для исследования эффективности многоуровневых систем защиты базовых информационных технологий использовать системный подход, базирующийся на теории случайных процессов [13, 14, 15,16]. На основе методов теории восстановления и аппроксимации используемых функций однопараметрическими распределениями предложен математический аппарат асимптотической теории для оценки защищенности информационных технологий в многоуровневых системах защиты, позволяющий получить простые аналитические формулы для оценки показателей защищенности информации от несанкционированного доступа (НСД) при использовании различных рубежей защиты, а также оперативно проводить системный анализ эффективности многоуровневых систем защиты в вычислительных системах различного назначения.

Изложение теоретических положений по оценке защищенности информационных технологий является достаточно универсальным и может быть полезно широкому кругу специалистов.

Основные положения теории восстановления, использующиеся для построения вероятностных моделей оценки защищенности информации от НСД.

Приведем основные положения теории восстановления [17, 18], которые будут использоваться при разработке аналитических методов оценки вероятностных показателей защищенности информации от НСД.

Определение 1. Последовательность моментов $t_к$, образованных независимыми случайными величинами $z_к = t_к - t_{к-1}$ ($z_1 = t_1, z_2 = t_2 - t_1, z_3 = t_3 - t_2, \ldots z_к = t_к - t_{к-1}$) с функцией распределения (ФР) $F_к(x)$, называется потоком с ограниченным последействием.

Определение 2. Если все $F_к(x)$, за исключением $F_1(x)$ совпадают,

т.е. $F_к(x) = F(x)$, $к \geq 2$, причем$F(+0) < 1$, говорят, что последовательность $\{t_к\}_{к=1}^{\infty}$ образует процесс восстановления.

Таким образом, процесс восстановления – более узкое понятие, нежели поток с ограниченным последействием.

$$F(x) = P\{z_к < x\} = F_к(x) \text{ (к = 2,3,....)}$$

Введем случайную величину N_t, равную числу восстановлений до момента *t*, т.е. наибольшее *n*, для которого

$$t_n = z_1 + z_2 + ... + z_n < t$$

Определение 3. Математическое ожидание случайной величины N_t называется функцией восстановления и обозначается символом

$H(t) = MN_t$.

Основные формулы для процессов восстановления.

Пусть *F(t)* - ФР интервалов восстановления $\{t_к\}$ $(к \geq 2), H(t)$ - функция восстановления.

Свойство 1

1. Пусть *u(t)* непрерывная ограниченная функция. Последовательности $\{t_n\}$ поставим в соответствие случайную функцию $\xi(t)$, где $\xi(t) = 0$ при $0 \leq t \leq t_1$, $\xi(t) = u(t - t_n)$ при $t_n \leq t < t_{n+1}$, $n \geq 1$.

Тогда

$$M\xi(t) = \int_0^t u(t-x)[1 - F(t-x)]dH(x) . \quad (1)$$

Предельная (узловая) теорема восстановления:

Пусть *Q(x)* – любая неотрицательная функция, определенная при положительных *x*, не возрастающая и интегрируемая в пределах $(0,\infty)$. При этих условиях имеет место следующая предельная теорема:

При

$$t \to \infty \int_0^t Q(t-u)dH(u) \to \frac{1}{a}\int_0^{\infty} Q(x)dx \text{, где } a = \int_0^{\infty} xdF(x) \quad (2)$$

Формализация и аналитическое описание модели процессов несанкционированного доступа к информационным и программным ресурсам.

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

i-го типа.

Рассмотрим оценку защищенности ресурсов *i*-го типа без учета периода их объективной ценности, т.е. лишь исходя из реализуемой технологии защиты. Другими словами, защищенные ресурсы полагаются априори ценными в течение бесконечного периода времени.

Формализация процессов несанкционированного доступа к ресурсам рассмотрена в работе [16].

Вероятность предотвращения НСД:

$$P_{защ(i)} = 1 - \prod_{m=1}^{\kappa} P_{НСД\ (m)}\ ,(3)$$

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

$P_{НСД(m)}$ - 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 $B_{конф\ (i)}(t)$.

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 защиты 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

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

$$\xi_m(t) = 0 \text{ при } 0 \le t < t_1$$

$\xi_m(t)$ в интервале $t_n \le t < t_{n+1}$, $(n \ge 1)$ 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

$$P_{НСД\ (m)} = M\xi_m(t) = \int_0^t \left\{\left[1 - F_{m\,i}(t-x)\right] U_{m\,i}(t-x)\right\} dH_m(x), \quad (4)$$

где $H_m(t)$ - функция восстановления.

В соответствии с предельной теоремой теории восстановления:

$$P_{НСД\ (m)} = \frac{1}{F_{mi}^{(1)}} \int_0^{\infty} \left[1 - F_{mi}(t)\right] U_{mi}(t)\,dt, \quad (5)$$

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

На 1-ом этапеприреализациимоделирующего комплекса ФР $F_{mi}(t)$ и $U_{mi}(t)$ выбираются в рамках аппроксимационной теории 1-го порядка из класса экспоненциальных или детерминированных функций. Поэтому для определения ФР $F_{mi}(t)$ и $U_{mi}(t)$ достаточно задать только математические ожидания этих ФР.

Формализация и вывод аналитических формул, описывающих модель сохранения конфиденциальности информации.

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 [16]:

$$P_{конф(i)} = 1 - \prod_{m=1}^{к} P_{НСД\ конф(m)}\ , (6)$$

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

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

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

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

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

$\xi_m(t) = U_{mi}(t - t_n) \cdot (1 - B_{конф(i)}(t - t_n))$ при $t_n \le t < t_{n+1}, n \ge 1$

$\xi_m(t) = 0$ при $0 \le t < t_1$

$\xi_m(t)$ в интервале $t_n \le t < t_{n+1} (n \ge 1)$ является вероятностью того, что период объективной конфиденциальности информации i-го типа ко времени t не истек $(1 - B_{конф(i)}(t - t_n))$ и нарушитель ко времени t расшифровал значения параметров информации m-ой преграды системы защиты информации i-го типа - $U_{m\ i}(t - t_m)$.

В соответствии со свойством 1 для процессов восстановления (формула 1)

$$P_{НСД\ конф(m)} = M\xi_m(t) = \int_0^t \left\{\left[1 - F_{m\,i}(t-x)\right] U_{m\,i}(t-x)(1 - B_{конф(i)}(t-x))\right\} dH(x), \quad (7)$$

где $H(x)$- функция восстановления.

В соответствии с предельной теоремой теории восстановления (2):

$$P_{НСД\ конф(m)} = \frac{1}{F_{mi}^{(1)}} \int_0^{\infty} \left[1 - F_{mi}(t)\right] U_{mi}(t)(1 - B_{конф(i)}(t))dt, \quad (8)$$

где $F_{mi}^{(1)}$ математическое ожидание ФР $F_{mi}(t)$.

Формула (8) справедлива, если $U_{mi}^{(1)} >> F_{mi}^{(1)}$ и $B_{конф(i)}^{(1)} >> F_{mi}^{(1)}$, то есть время расшифровки параметров m-ой преграды системы защиты информации i-го типа и период объективной конфиденциальности намного больше времени между соседними изменениями m-ой преграды системы защиты параметров информации i-го типа.

В том случае, когда на параметры ФР $B_{конф\ (i)}(t)$ и $U_{mi}(t)$ не накладывается ограничений, а предполагается только, что $B_{конф\ (i)}(t)$ принадлежит классу экспоненциальных ФР, последовательности точек регенерации $\{t_n\}$ должна ставиться в соответствие случайная функция $\xi(t)$, при построении которой используется дифференциальный подход:

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

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

В соответствии со свойством 1 для процессов восстановления

$$P_{НСД\ конф(m)} = M\xi_m(t) = \int_0^t \left\{\left[1 - F_{mi}(t-x)\right] \int_0^{t-x} (1 - B_{конф(i)}(\theta))dU_{mi}(\theta)\right\} dH(x), \quad (9)$$

и в соответствии с предельной теоремой теории восстановления

$$P_{НСД\ конф(m)} = \frac{1}{F_{mi}^{(1)}} \int_0^{\infty} \left\{\left[1 - F_{mi}(t)\right] \int_0^t \left[dU_{mi}(\theta) \cdot (1 - B_{конф(i)}(\theta))\right]\right\} dt. \quad (10)$$

При разработке программных продуктов, предназначенных для оценки $P_{конф(i)}$ (формулы (6) - (10)), в первом приближении (в рамках теории
1-го порядка) целесообразно выбирать ФР $F_{mi}(t)$, $U_{mi}(t)$ из класса экспоненциальных и детерминированных.

На первом этапе для проведения практических расчетов по оценке вероятности сохранения конфиденциальности информации предполагается использовать моделирующий комплекс с оконным интерфейсом «КОК» [16].

Несанкционированный доступ к ресурсам i-го типа.

Вероятность предотвращения НСД к ресурсам i-го типа при использовании многоуровневых систем защиты определяется соотношением (3):

Вероятность преодоления нарушителем m-й преграды $P_{НСД_{(i)m}}$ в соответствии с формулой (5) равна:

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

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** $U_{(i)m}(t)$**:**

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

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

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

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

$$\mathrm{P_{НСД_{(i)m}}} = \frac{1}{\mathrm{f_{(i)m}}} \frac{f_{(i)m}^2}{f_{(i)m} + u_{(i)m}} = \frac{f_{(i)m}}{f_{(i)m} + u_{(i)m}} = \frac{\frac{1}{u_{(i)m}}}{\frac{1}{f_{(i)m}} + \frac{1}{u_{(i)m}}} \quad (11)$$

$$\mathrm{P_{защ(i)m}} = 1 - \mathrm{P_{НСД_{(i)m}}} = 1 - \frac{\frac{1}{u_{(i)m}}}{\frac{1}{f_{(i)m}} + \frac{1}{u_{(i)m}}} = \frac{\frac{1}{f_{(i)m}}}{\frac{1}{f_{(i)m}} + \frac{1}{u_{(i)m}}} = \frac{u_{(i)m}}{f_{(i)m} + u_{(i)m}} \quad (12)$$

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

$$U_{(i)m}(t) = 1 - \exp(-t * u_{(i)m}^{-1}),$$

$$u_{(i)m} = \int_0^{\infty} t dU_{(i)m}(t)$$

$$F_{(i)m}(t) = \begin{cases} 0, \circ npu \circ t \le f_{(i)m} \\ 1, \circ npu \circ t > f_{(i)m} \end{cases},$$

$$f_{(i)m} = \int_0^{\infty} t dF_{(i)m}(t)$$

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

$$\mathrm{P}_{\mathrm{НСД}_{(i)m}} = \frac{1}{\mathrm{f}_{(i)m}} \int_0^{\infty} [1 - \mathrm{F}_{(i)m}(t)] \mathrm{U}_{(i)m}(t) dt = \frac{1}{\mathrm{f}_{(i)m}} \int_0^{f_{(i)m}} 1 * [1 - \exp(-t / u_{(i)m})] dt$$

$$\mathrm{P}_{\mathrm{НСД}_{(i)m}} = \frac{1}{\mathrm{f}_{(i)m}} \{ f_{(i)m} - u_{(i)m} [1 - \exp(-f_{(i)m} / u_{(i)m})] \} =$$

$$= 1 - \frac{u_{(i)m}}{f_{(i)m}} [1 - e^{-\frac{f_{(i)m}}{u_{(i)m}}}] \qquad (13)$$

$$\mathrm{P}_{\text{защ(i)m}} = 1 - \mathrm{P}_{\mathrm{НСД}_{(i)m}} = \frac{u_{(i)m}}{f_{(i)m}} [1 - e^{-\frac{f_{(i)m}}{u_{(i)m}}}] \quad (14)$$

Несанкционированный доступ к ресурсам i-го типа в течение заданного директивного периода.

Вероятность предотвращения НСД к ресурсам i-го типа в течение заданного периода времени $P_{конф(i)}$ равна (см. формулы (6) и (10)):

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

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):

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

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*** $U_{(i)m}(t)$**:**

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

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

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

Следовательно

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

$$dU_{(i)m}(\theta) = \frac{1}{u_{(i)m}} \exp(-\theta / u_{(i)m}) d\theta,$$

тогда:

$$\int_0^t [1 - B_{конф(i)}(\theta)] dU_{(i)m}(\theta) = \int_0^t \frac{1}{u_{(i)m}} e^{-\theta / u_{(i)m}} e^{-\theta / h_{(i)}} d\theta =$$

$$= \frac{\frac{1}{u_{(i)m}}}{\frac{1}{u_{(i)m}} + \frac{1}{h_{(i)}}} - \frac{\frac{1}{u_{(i)m}}}{\frac{1}{u_{(i)m}} + \frac{1}{h_{(i)}}} \exp\left(-t\left(\frac{1}{u_{(i)m}} + \frac{1}{h_{(i)}}\right)\right)$$

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

$$-\frac{\frac{1}{u_{(i)m}}}{\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}}\int_0^{\infty}e^{-t\left(\frac{1}{f_{(i)m}}+\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)m}}\right)}dt=f_{(i)m}\frac{\frac{1}{u_{(i)m}}}{\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}}\{1-\frac{\frac{1}{f_{(i)m}}}{\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}+\frac{1}{f_{(i)m}}}\}$$

$$P_{НСДконф(i)m}=\frac{\frac{1}{u_{(i)m}}}{\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}}\{1-\frac{\frac{1}{f_{(i)m}}}{\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}+\frac{1}{f_{(i)m}}}\}=\frac{\frac{1}{u_{(i)m}}}{\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}+\frac{1}{f_{(i)m}}}\quad(15)$$

$$P_{ЗАЩконф(i)m}=1-P_{НСДконф(i)m}=\frac{\frac{1}{h_{(i)}}+\frac{1}{f_{(i)m}}}{\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}+\frac{1}{f_{(i)m}}}\quad(16)$$

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

$$U_{(i)m}(t)=1-\exp(-t*u_{(i)m}^{-1}),\ u_{(i)m}=\int_0^{\infty}tdU_{(i)m}(t)$$

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

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

В этом случае получим:

$$\int_0^{t}\left[1-B_{\text{конф(i)}}(\theta)\right]\text{dU}_{\text{(i)m}}(\theta)=$$

$$= \frac{\frac{1}{u_{(i)m}}}{\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}} - \frac{\frac{1}{u_{(i)m}}}{\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}} \exp(-t(\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}))$$

$$\int_0^{\infty}\{[1-F_{(i)m}(t)]\int_0^{t}[1-B_{\text{конф(i)}}(\theta)]\text{dU}_{\text{(i)m}}(\theta)\}\text{dt} = \frac{\frac{1}{u_{(i)m}}}{\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}}\int_0^{f_{(i)m}} dt -$$

$$-\frac{\frac{1}{u_{(i)m}}}{\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}}\int_0^{f_{(i)m}} e^{-t(\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}})}dt = f_{(i)m}\frac{\frac{1}{u_{(i)m}}}{\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}} - \frac{\frac{1}{u_{(i)m}}}{(\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}})^2} +$$

$$+\frac{\frac{1}{u_{(i)m}}}{(\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}})^2}\exp\{-f_{(i)m}(\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}})\}$$

$$P_{НСДконф(i)m} = \frac{\frac{1}{u_{(i)m}}}{\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}}} + \frac{\frac{1}{u_{(i)m}} * \frac{1}{f_{(i)m}}}{(\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}})^2}[\exp\{-f_{(i)m}(\frac{1}{u_{(i)m}}+\frac{1}{h_{(i)}})\}-1] \quad (17)$$

$$P_{ЗАЩконф(i)m} = 1 - P_{НСДконф(i)m} \quad (18)$$

Таким образом, формулы (11), (12), (13), (14) позволяют рассчитать защищенность i-ых ресурсов системы m-ой преградой от НСД, а формулы (15), (16), (17), (18) – 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 в рамках асимптотической теории 1-го порядка.

Заключение.

Перечислим основные полученные результаты:

1. Рассмотрены вопросы использования аналитических моделей для оценки защищенности информационных технологий.

2. На основе методов теории восстановления и однопараметрической аппроксимации используемых функций распределения разработан математический аппарат аналитической теории первого порядка (асимптотической теории) для оценки защищенности информационных технологий при использовании многоуровневых систем защиты.

3. Полученные формулы для оценки защищенности информационных технологий позволяют проводить системный многовариантный анализ параметров многоуровневых систем защиты в различных информационно-вычислительных системах и выбирать рациональные варианты защиты, удовлетворяющие требованиям заказчика.

4. Изложенные материалы нашли практическое применение при оценке эффективности защиты информационных технологий на основе инструментально-моделирующего комплекса КОК в вычислительных системах различного назначения.

5. Изложение теоретических положений по оценке защищенности информационных технологий является достаточно универсальным и может быть полезно широкому кругу специалистов.

Использованные источники:

1. Нестеров С.А. Основы информационной безопасности. – Спб.: Лань, 2021. – 324 с.
2. Суворова Г.М. Информационная безопасность// Учебное пособие для вузов. – М.: Издательство Юрайт, 2021. – 253 с.
3. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика. Электроинформ, 2016. – 368 с.
4. Леонтьев А.С. Защита информации// Учебное пособие. Электронное издание. № госрегистрации 0322102783. –М.: МИРЭА – Российский технологический университет, 2021. – 84 с.
5. Константинов В.П., Юхневич Л.А. Безопасность автоматизированных систем обработки информации и управления// Учебное пособие. – М.: МИРЭА, 2007. 91 с.
6. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками// Учебное пособие для вузов. – М.: Горячая линия – Телеком. – 2013. – 338 с.
7. Буйневич М.В., Покусов В.В., Израилов К.Е. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации// Информатизация и связь. – 2021, № 4. – С. 66-73.
8. Лифшиц И.И. Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами: дисс. доктора техн. наук: 05.13.19/ СПИИРАН. – Санкт-Петербург. – 2018. – 407 с.

9. Миняев А.А. Методика оценки эффективности системы защиты территориально-распределенных информационных систем: дисс. канд. техн. наук: 2.3.6 / Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. – Санкт-Петербург. – 2021. – 216 с.
10. Коломойцев В.С. Модели и методы оценки эффективности систем защиты информации и обоснование их комплектации: дисс. канд. техн. наук: 05.13.19/ Университет ИТМО. – Санкт-Петербург. – 2018. -175 с.
11. Маркин Д.О., Комашинский В.В., Сенотрусов И.А. Методика оценки эффективности защиты информации при эксплуатации мобильных абонентских устройств в корпоративных сетях с разнородными требованиями по защищенности// Вопросы кибербезопасности. 2017, № 4(22) – С. 21-31. DOI: 10.21681/2311-3456-2017-4-21-31.
12. Использование численно-аналитической модели оценки эффективности функционирования системы защиты информации от несанкционированного доступа при анализе ее вероятностно-временных характеристик/
В.П. Алферов, А.В. Бацких, А.В. Крисилов, А.Д.Попов, Е.А. Рогозин// Вестник Дагестанского государственного университета. Технические науки. 2020. 47(1): 58-71. DOI: 10.21822/2073-6185-2020-47-1-58-71.
13. 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.
14. Гусев К.В., Леонтьев А.С. Теоретическое развитие моделей для оценки защищенности от несанкционированного доступа и сохранения конфиденциальности используемой информации // ИТ Стандарт, 2021. № 4(29). – С. 38-44. URL: htpp://journal.tc22.ru.
15. Леонтьев А.С., Рожицкая П.Д. Аналитические методы оценки вероятностных показателей защищенности информационных технологий от несанкционированного доступа // Учебное пособие. Электронное издание. № госрегистрации 0321803742. – М.: МИРЭА, 2018. – 55 с.
16. 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.
17. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. М.: Наука. Гл. ред. физ.-мат. лит. – 1987. – 336с.

18. Климов Г.П. Стохастические системы обслуживания. – М.: Наука, 1966. – 244 с.