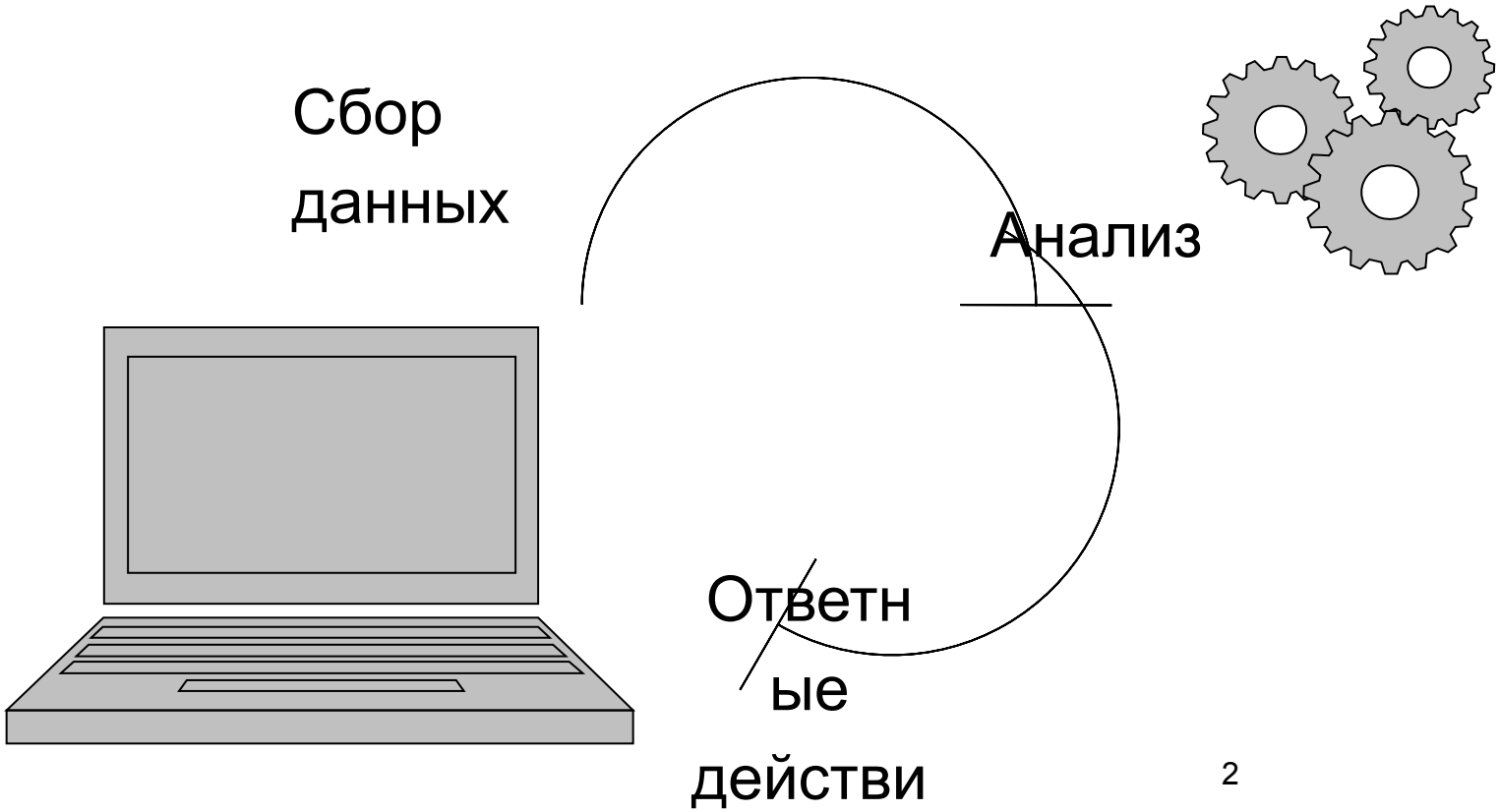
Система активного аудита: методы выявления аномальной активности

К.К. Маркелов (НИИМЕХ МГУ)

09.10.2007

Введение

Задачей системы активного аудита является сбор данных о состоянии анализируемой компьютерной системы, их анализ и принятие на основе анализа (в случае необходимости) ответных действий.



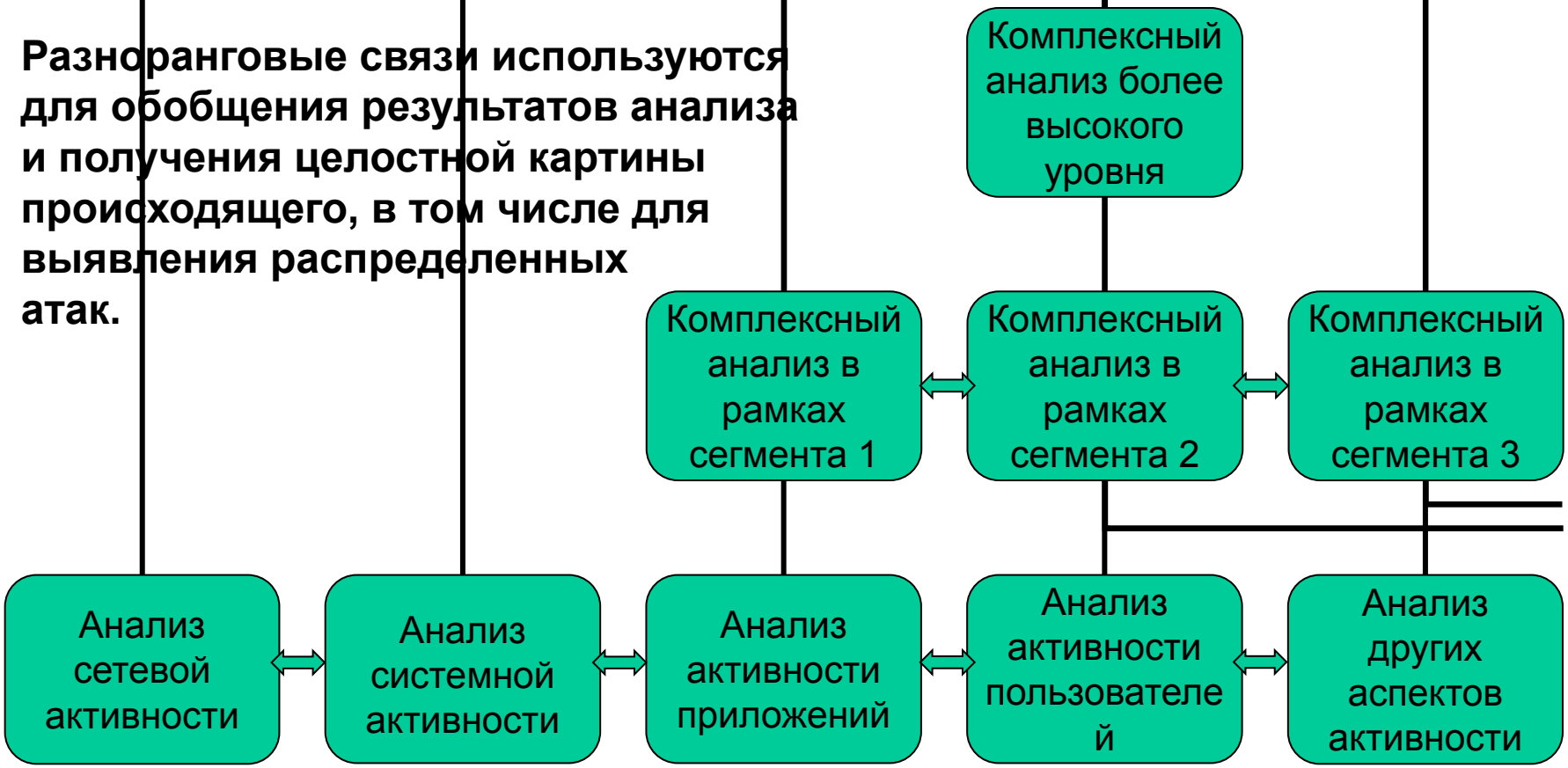
Введение

Необходимость использования подобных систем обусловлена рядом причин:

- **недостаточность возможностей механизмов безопасности, заложенных в операционных системах и поддерживаемых стандартными программными средствами;**
- **возможность человеческих ошибок при администрировании системы;**
- **возможность появления новых, неизвестных уязвимостей в программном обеспечении.**

Глобальная архитектура распределенной САА

Разноранговые связи используются для обобщения результатов анализа и получения целостной картины происходящего, в том числе для выявления распределенных атак.



Методы обнаружения вторжений

- Поиск известных атак
  - Сигнатурные методы
- Поиск аномальной активности
  - Статистические методы
  - Нейросетевые методы
  - Распознавание образов

Методы обнаружения вторжений

- **Сигнатурный анализ**

Достоинства

- низкий уровень ложных тревог
- простота осуществления
- точность обнаружения

Недостатки

- пропуск неизвестных атак
- поддержка базы сигнатур

- **Поиск аномалий**

Достоинства

- возможность обнаружения новых атак
- отсутствие необходимости поддерживать и обновлять базу сигнатур

Недостатки

- высокий уровень ложных тревог
- отсутствие обоснования реагирования

Оптимальная конфигурация системы активного аудита может быть достигнута совместным использованием обоих методов.

Основные сложности и недостатки статистического анализа

- генерация относительно большого количества ложных тревог;
- сложность учета изменчивости контролируемой компьютерной системы;
- сложность учета изменчивости поведения части пользователей;
- отсутствие четкого обоснования тревог;
- возможность внедрения, злонамеренной активности в шаблон нормального поведения в период установки системы;
- отсутствие немедленного эффекта при установке;
- технические проблемы, связанные с правильным конфигурированием системы

Простейшие методы статистического анализа, применяемые на практике.

- 1. Операционная модель основывается на том, что каждое новое наблюдение переменной должно укладываться в некоторых границах.
- 2. Модель среднего значения и среднеквадратичного отклонения.
- 3. Многовариационная модель аналогична модели среднего значения и среднеквадратичного отклонения, но учитывает корреляцию между двумя или большим количеством метрик.
- 4. Модель Марковского процесса применима только к счетчикам событий, рассматривая каждый тип событий как переменную состояния и используя матрицу переходов для характеристики частот переходов между состояниями.
- 5. Модель временных серий использует временные периоды вместе с счетчиками событий и измерениями ресурсов.

Примеры систем статистического анализа

- SPADE

P(dip=198.168.1.1,dport=80)= 0.3
P(dip=198.168.1.1,dport=12543) =0.001.

Оценка аномальности рассчитывается непосредственно из вероятности появления пакета:

$$A(x) = -\log_2 (P(x)) .$$

- EMERALD

Система eBayes (EMERALD) посредствам создания и проверки статистических гипотез нормального поведения системы, нападения, и аномального поведения. Система eBayes собирает некоторые параметры открывшихся соединений сети (например максимальное число открытых связей с любым отдельным хостом), затем на основе вероятностных методов, отвергает или принимает гипотезу о нормальности соединения.

Использование статистических критериев

- исследуемые характеристики имеют категориальную природу
- долгосрочные и краткосрочные профили представляют собой гистограммы распределений
- нетипичное поведение представлено произвольным распределением, отличным от заданного

Примеры использования статистических критериев

- R. Lippmann, J.W. Haines, D.J. Fried, J. Korba and K. Das, The 1999 DARPA Off-Line Intrusion Detection Evaluation, Computer Networks, 2000. - Описаны успешные результаты тестирования критерия Колмогорова-Смирнова для выявления злонамеренных telnet-соединений.
- N. Ye and Q. Chen, An Anomaly Detection Technique Based on a Chi-Square Statistic for Detecting Intrusions Into Information Systems, Quality and Reliability Engineering International, vol. 17, 2, pp. 105-112, 2001. Описаны успешные результаты использования критерия хи-квадрат, предложен подход, где деятельность в системе представлена через поток событий, который затем классифицируется по типам. Для каждого типа события, определены профили нормального поведения.

Основные теоретические задачи

- Основная проблема – оценка адекватности работы анализатора. Под этим подразумевается определение априорных свойств тех или иных методов принятия решений. Например, можно, искать максимум вероятностей ошибок анализатора по всем возможным распределениям активности и всем возможным наблюдениям.
- Задание эффективного порогового значения – отдельная содержательная задача, которая может решаться, например, минимизацией взвешенной суммы ошибок анализатора. Аналогичный подход может быть применен для решения проблемы выбора оптимального критерия.
- При выявлении очередной аномалии необходимо определить степень доверия принятому решению, а именно определить вероятность, с которой данное решение может является ошибочным.

Формализация поиска аномалий

Пусть дана выборка $X = (x_1, \ldots, x_n)$ из распределения F.

Опр. Гипотезой H называется любое предположение о распределении наблюдений: $H = \{F = F_1\}$ *или* $H = \{F = \hat{F}\}$.

Опр. Если имеются гипотезы $H_1, H_2, \ldots, H_k$, *то нерандомизированным критерием* $\delta = \delta(x_1, x_2, \ldots, x_n)$ *называется отображение* $\delta : R^n \to \{H_1, H_2, \ldots, H_k\}$.

Опр. Для заданного критерия будем говорить, что произошла ошибка i-го рода, если гипотеза H_i *отвергнута критерием, в то время как она верна. Вероятностью ошибки i-го рода критерия* δ *называется* $\alpha_i(\delta) = \mathrm{P}_{H_i}(\delta(X) \neq H_i)$.

Критическая область

Для пришедшего на вход анализатору набора данных $(x_1,\ldots,x_n)$ описываем функцию распределения F_X, соответствующую этому набору, строим простую гипотезу $H_0=\{F_X=F\}$ и сложную альтернативу $H_1=\{F_X\neq F\}$. Таким образом, необходимо выяснить, верна гипотеза "атак нет", или альтернатива "система под угрозой".

Каков бы ни был критерий $\delta(X): R^n \to \{H_0, H_1\}$, он принимает не более двух значений. То есть область R^n делится на две части $R^n = S \cup (R^n \setminus S)$ так, что $\delta(X)=\begin{cases} H_0, \text{ если } X \in R^n \setminus S, \\ H_1, \text{ если } X \in S. \end{cases}$

Область S, в которой принимается вторая (альтернативная) гипотеза, называют критической областью.

Ошибки первого и второго рода

Опр. Вероятность ошибки первого рода $\alpha_1 = \alpha_1(\delta)$ *называют размером или уровнем значимости критерия* δ *:*

$$\alpha_1(\delta) = \mathrm{P}_{H_1}\left(\delta(X) \neq H_1\right) = \mathrm{P}_{H_1}\left(\delta(X) = H_2\right) = \mathrm{P}_{H_1}\left(X \in S\right).$$

Мощностью критерия δ *называют величину* $1-\alpha_2$*, где* $\alpha_2 = \alpha_2(\delta)$ *- вероятность ошибки второго рода критерия* δ *. Мощность критерия равна*

$$1-\alpha_2(\delta) = 1-\mathrm{P}_{H_2}\left(\delta(X) \neq H_2\right) = \mathrm{P}_{H_2}\left(\delta(X) = H_2\right) = \mathrm{P}_{H_2}\left(X \in S\right).$$

В случае обнаружения вторжений α_1— это вероятность ложной тревоги, α_2 — это вероятность пропуска атаки. Ущерб, нанесенный информационно-вычислительному комплексу в случае пропуска той или иной атаки, то есть в случае допуска системой активного аудита ошибки второго рода - C_{α_2} . Ущерб в случае ложного срабатывание системы C_{α_1}. Можно поставить математическую задачу выбора критического множества, с целью минимизации общего возможного ущерба $\alpha_1 C_{\alpha_1} + \alpha_2 C_{\alpha_2}$

Классический критерий хи-квадрат

Согласно выбранной концепции, зададим приемлемую для нас ошибку первого рода ϵ. Пусть z_ϵ - ϵ-квантиль функции распределения χ^2, то есть решение уравнения $\epsilon = F(z)$, где $F(z)$ - функция распределения χ^2 с k степеням свободы.

$$F(z) = \frac{1}{2^{k/2}\Gamma(k/2)} \int_0^z z^{\frac{k}{2}-1} e^{-\frac{z}{2}} dz$$

Согласно формуле $Q = N \sum_{i=1}^{k} \frac{\left(P_i' - P_i\right)^2}{P_i}$ считаем статистику Q. Если $Q < z_\epsilon$, для $k-1$ степеней свободы, то гипотеза принимается. То есть наблюдаемые частоты событий не являются аномальными. В противном случае, гипотеза отвергается и принимается альтернатива.

Описание критического множества для критерия хи-квадрат

$$|P'_i - P_i| < \sqrt{\frac{z_\epsilon P_i}{Nk}} \quad \forall i.$$

Определение. Множество P'_i, удовлетворяющее этому неравенству будем называть "вероятностной трубкой" графика функции распределения F_0 (гистограммы, построенной по значениям P_i) с относительным диаметром $\sqrt{\frac{z_\epsilon P_i}{Nk}}$.

Утверждение. Если гистограмма значений P'_i лежит полностью в указанном множестве, то анализатор будет считать, что система находится в безопасном состоянии.

Оценка качества критерия

$\alpha_2 = \alpha_2(\delta)$ - вероятность ошибки второго рода критерия δ. Мощность критерия равна $1 - \alpha_2(\delta) = 1 - \mathrm{P}_{H_2}(\delta(X) \neq H_2) = \mathrm{P}_{H_2}(\delta(X) = H_2) = \mathrm{P}_{H_2}(X \in S) = P_{H_2}(Q > z_\epsilon)$.

Последнее равенство верно для используемого критерия. Чтобы примерно оценить это значение можно подсчитать по следующей формуле

$$\frac{1}{M}\sum_{j=1}^{M} I_{\{Q_j < z_\epsilon \mid H_2\}}$$

Операционная модель

$\alpha = P_{\bar{x}}(y \geq \bar{x} + d) + P_{\bar{x}}(y \leq \bar{x} - d)$

Вероятность пропуска атаки на значении y есть

$\beta = 1 - P_M(y > \bar{x} + d) - P_M(y < \bar{x} - d)$

Далее пользуемся определением функции распределения и получаем следующую теорему.

Теорема. В операционной модели с параметрами $\bar{x}$ и d ошибки первого и второго рода выражаются через функции распределения следующим образом:

$$\alpha = 1 - F(\bar{x} + d) + F(\bar{x} - d)$$

$$\beta = \tilde{F}(\bar{x} + d) - \tilde{F}(\bar{x} - d)$$

Модель среднего значения

Теорема. Пусть в дискретной модели среднего значения математическое ожидание «нормального» значения параметра активности есть M_1, *а аномального —* M_2; *решающим правилом является сравнение с пороговым значением* L *(для определенности будем считать* $M_1 < M_2$, *в этом случае значение параметра активности считается «нормальными», если оно меньше* L. *В случае* $M_1 > M_2$ *— если оно больше* L*). Тогда, условие* $M_1 \le L-1 < L \le M_2$, *гарантирует, что какими бы ни были распределения вероятностей, соответствующие* M_1 *и* M_2, *ошибки первого и второго рода не превысят соответственно* $(M_1-1)/(L-1)$ *и* $(n-M_2)/(n-L+1)$, *и при этом на некоторых распределениях ошибки могут достигать* 0.

Если $M_1 > L-1$, *то* $\alpha \ge (M_1 - L+1)/(n-L+1)$.

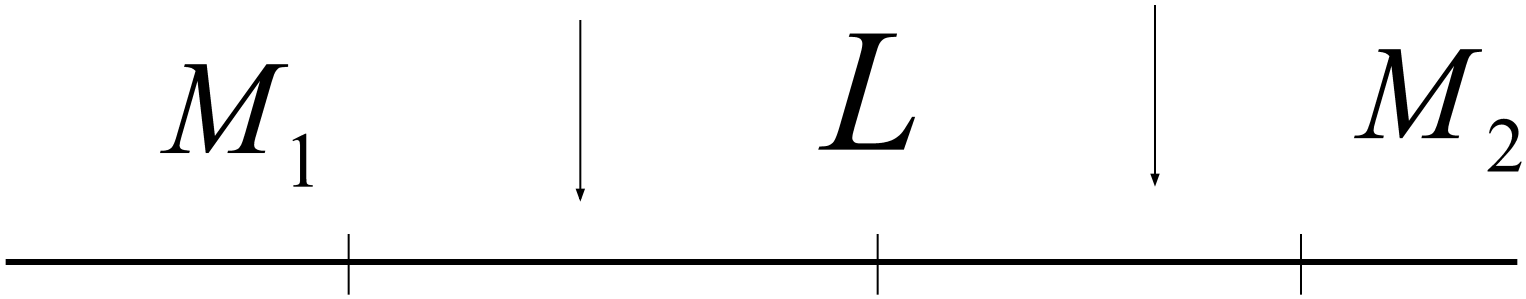
Если же $M_1 > L$, *то на некоторых распределениях ошибка первого рода будет достигать* 1.

Если $M_2 < L$, *то* $\beta \ge (L-M_2)/(L-1)$.

Если же $M_2 < L-1$, *то на некоторых распределениях ошибка второго рода будет достигать* 1.

Модель среднего значения

$$\beta \le \frac{n - M_2}{n - L + 1} \qquad \alpha \le \frac{M_1 - 1}{L - 1}$$



$$M_1 \le L - 1 < L \le M_2$$

Методы объединения частных показателей аномального поведения

$A_1, A_2, ..., A_n$ - n показателей аномального поведения (0 или 1).

I – гипотеза, констатирующая, что в данный момент система подвергается умышленной атаке. Тогда по теореме Байеса:

$P(A_i \mid I)$ достоверность

$P(A_i \mid \neg I)$ чувствительность

$$P(I \mid A_1, A_2, ..., A_n) = \frac{P(A_1, A_2, ..., A_n \mid I) \cdot P(I)}{P(A_1, A_2, ..., A_n)}$$

Если предположить независимость

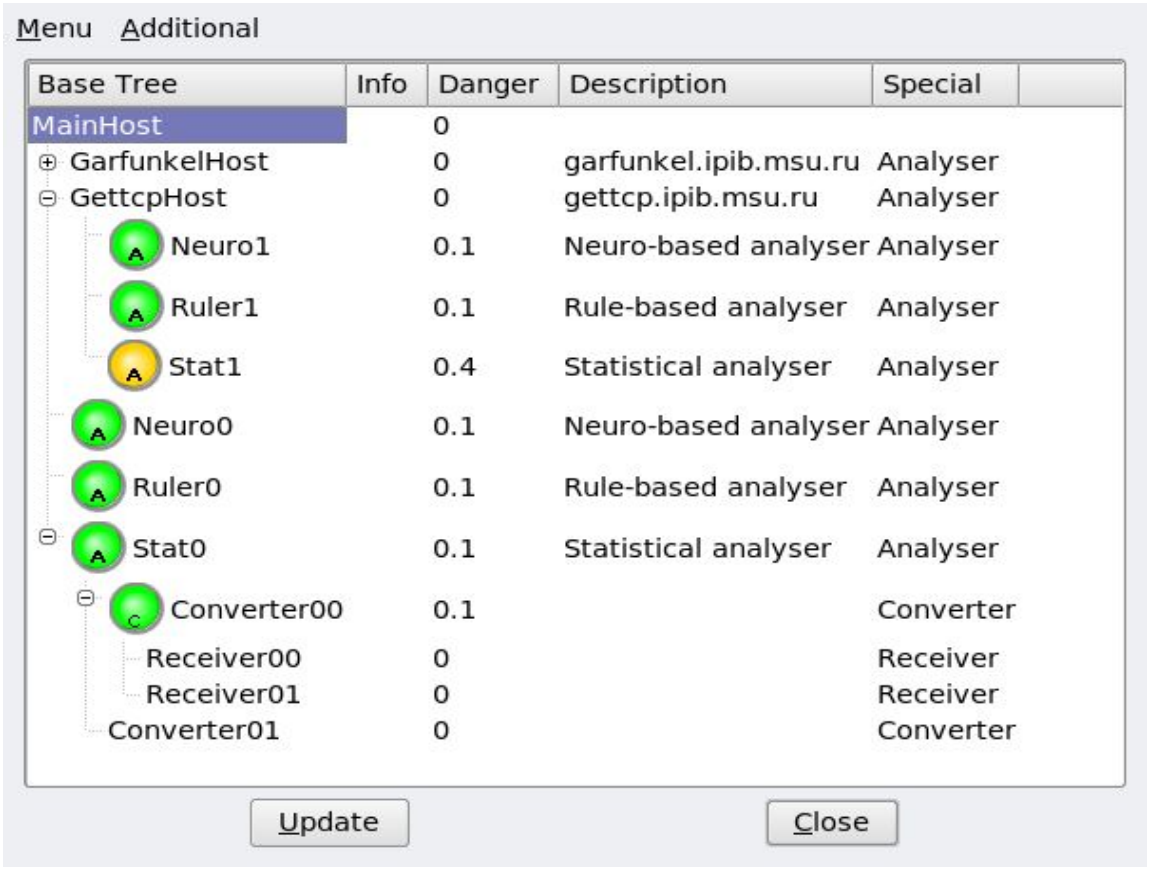
$$\mathrm{P}\left(A_1, A_2, ..., A_n \middle| I\right) = \prod_{i=1}^{n} P\left(A_i \middle| I\right)$$

$$\frac{\mathrm{P}\left(I \middle| A_1, A_2, ..., A_n\right)}{\mathrm{P}\left(\neg I \middle| A_1, A_2, ..., A_n\right)} = \frac{\mathrm{P}(I) \cdot \prod_{i=1}^{n} \mathrm{P}\left(A_i \middle| I\right)}{\left(\mathrm{P}(\neg I) \cdot \prod_{i=1}^{n} \mathrm{P}\left(A_i \middle| \neg I\right)\right)}$$

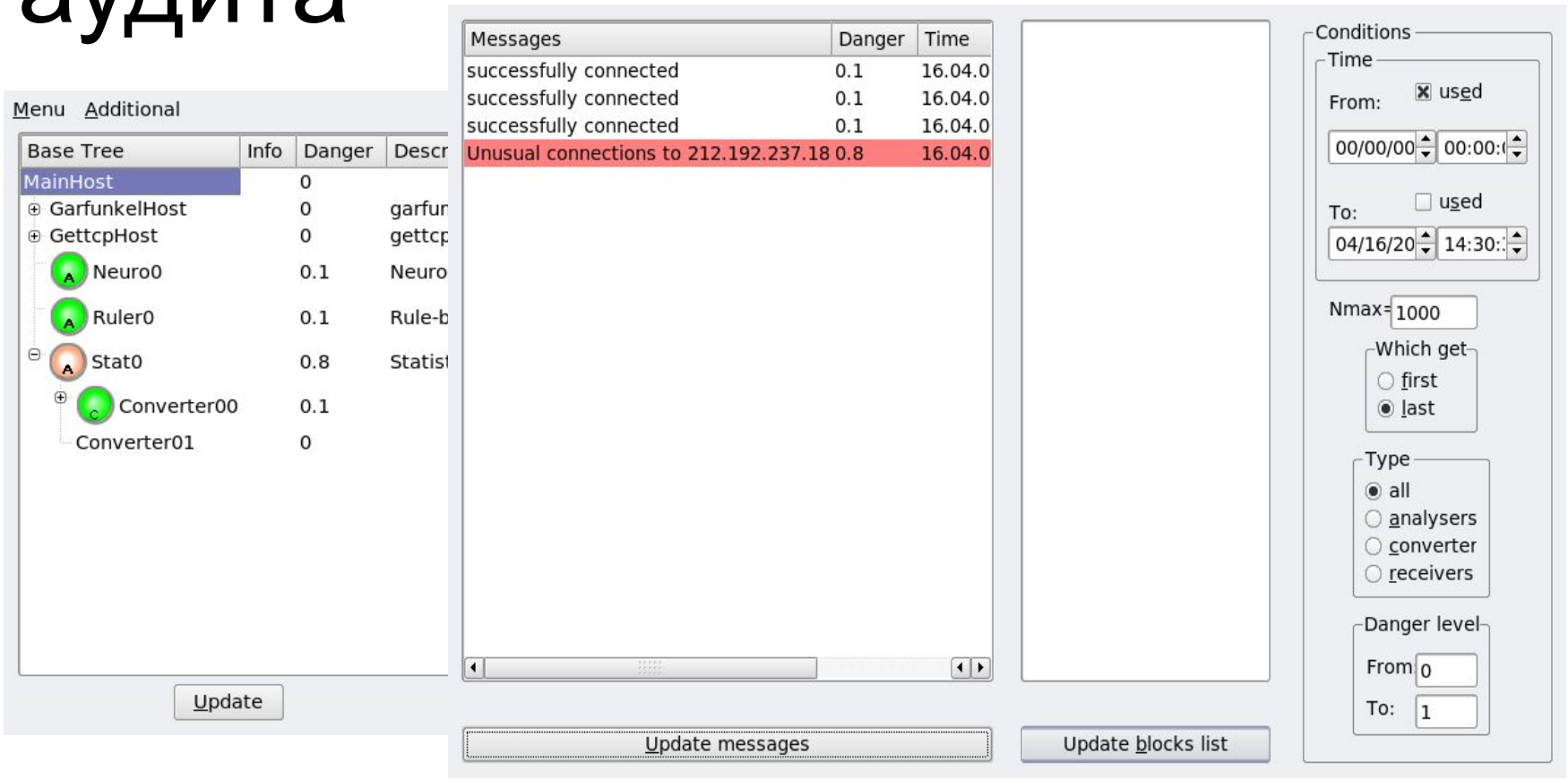
Основные требования к программным средствам выявления аномальной активности

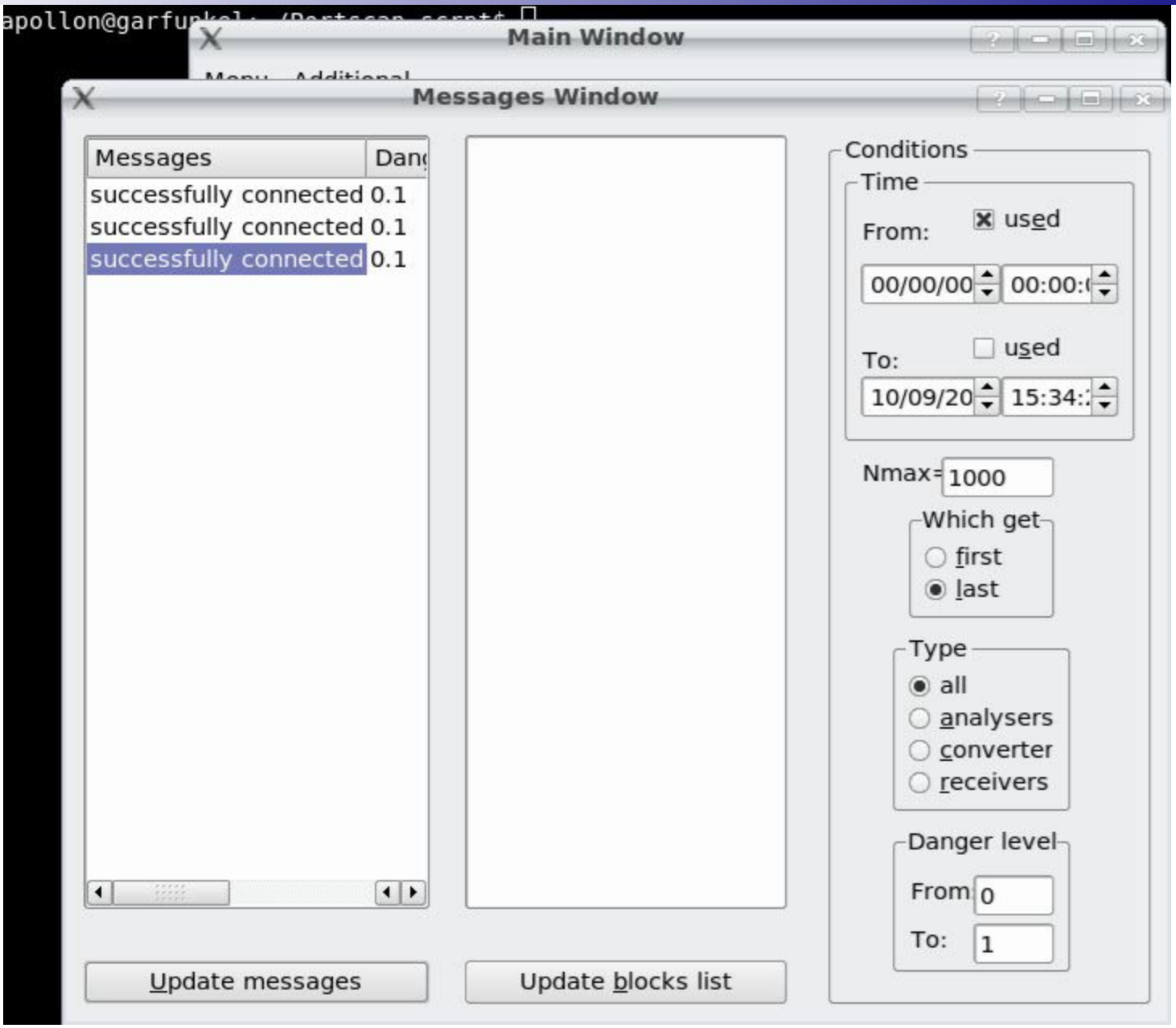
- модуль должен обладать теоретическими свойствами:
  - адекватность работы в рамках построенной модели;
  - оптимальность порогового значения;
- модуль должен обладать практическими свойствами:
  - способность анализа абстрактных типов данных;
  - обладать более гибкой настройкой, чем существующие решения;
  - способность автоматической адаптации к изменчивости защищаемой системы;
  - обладать четким обоснованием атак

Прототип системы активного аудита



Прототип системы активного аудита




Main Window
Messages Window
Messages
successfully connected 0.1
successfully connected 0.1
successfully connected 0.1
Conditions
Time
From:
used
00/00/00
To:
used
10/09/20
Nmax=
1000
Which get
first
last
Type
all
analysers
converter
receivers
Danger level
From
0
To:
1
Update messages
Update blocks list

Спасибо за внимание

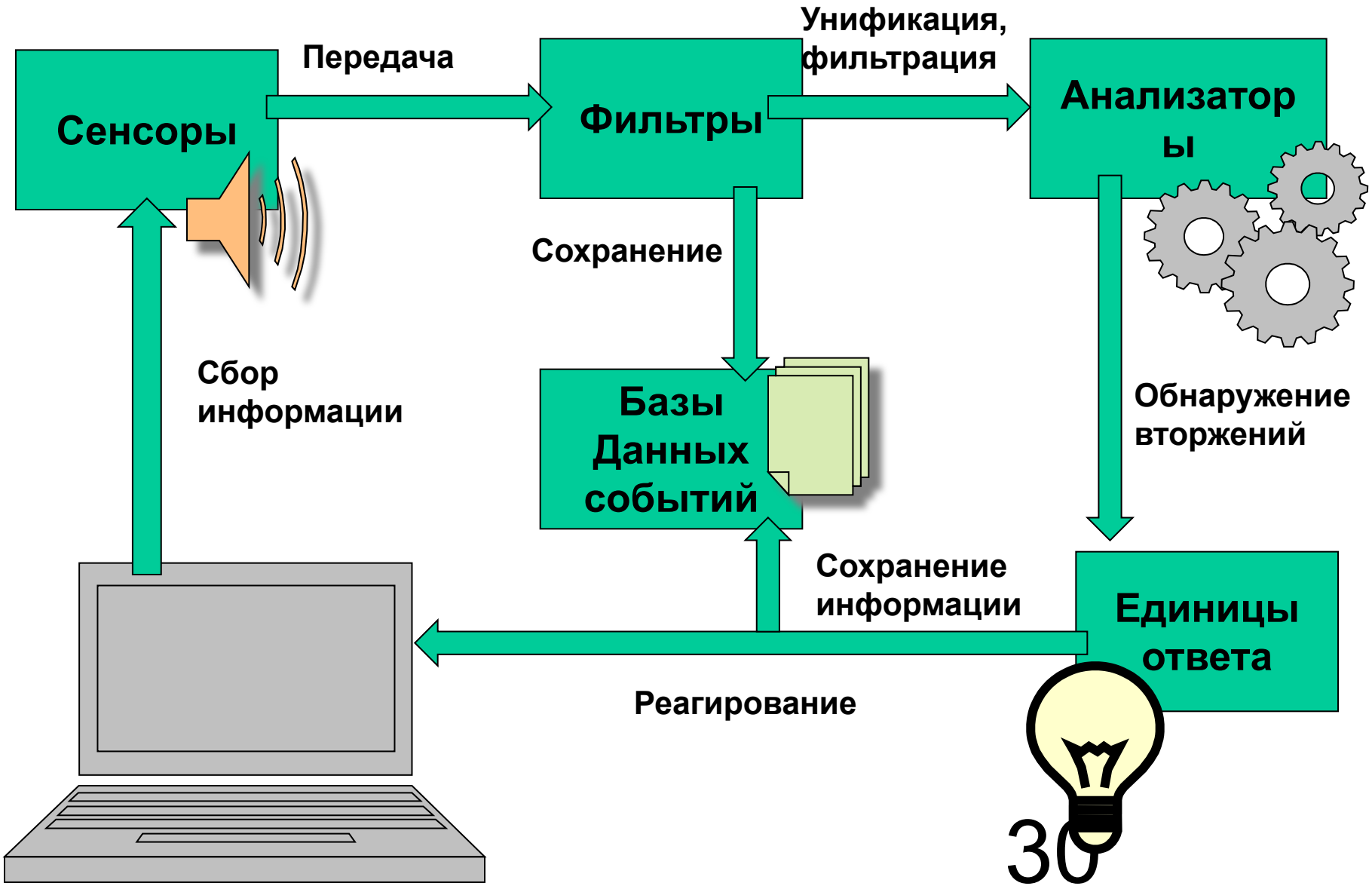
Дальнейшая работа

- дальнейшее развитие построенной модели;
- дальнейший анализ применимости статистических критериев с практической точки зрения;
- реализация методов объединения частных показателей аномального поведения и развитее моделей доверительных сетей;
- расширение функциональности системы;
- создание среды тестирования системы активного аудита.

Полученные результаты

- проведен анализ существующих подходов к обнаружению вторжений;
- формализована модель обнаружения аномальной активности;
- получены теоретические результаты для некоторых методов статистического анализа;
- реализованы модули статистического анализа системы активного аудита, опираясь на полученные математические результаты;
- реализован набор вспомогательных модулей системы активного аудита: сетевой сенсор, парсер регистрационных журналов ОС UNIX, сенсор использования системных ресурсов, шаблонный фильтр.

Локальная архитектура



Меры аномальности

Критерий Колмогорова-Смирнова Данный критерий применяется при проверках гипотезы однородности функций распределения против альтернативы неоднородности $F(x) \neq G(x)$ в некоторой окрестности точки x_0.

Мерой различия функций распределений служит следующая статистика:

$$D = sup_x|F(x) - G(x)|$$

Критерий Манна-Уитни Данный критерий применяется к двум выборкам любой длины. Критерий, в первую очередь, предназначен для проверки гипотезы совпадения функций распределения против правосторонней: $(F < G)$ и левосторонней $(F > G)$ альтернатив.

По определению, статистика Манна-Уитни имеет вид:

$$U = \sum_{i,j} I_{\{x_i < y_j\}}$$

Меры аномальности

Критерий омега-квадрат Для критерия омега-квадрат мерой аномальности служит величина

$$\omega_n{}^2 = \int_{+\infty}^{-\infty} \left[\hat{F}_n(x) - F(x)\right]^2 \psi[F(x)]dF(x),$$

где $\psi(y)$ — заданная на $[0,1]$ весовая функция. Рассмотрим 2 варианта:

$\psi_1 = 1$ — критерий Крамера-Мизеса,

$\psi_2(y) = 1/[y(1-y)]$ — критерий Андерсона-Дарлинга.

Первый из них рассчитан на отлов расхождений функций распределений в области «типичных значений» F (Часто оказывается более чувствительным, чем критерий Колмогорова-Смирнова). Второй критерий благодаря тому, что $\psi_2(y)$ быстро возрастает при $y- > 0$ и $y- > 1$, способен заметить различие «на хвостах» F, это означает, что этот критерий более чувствителен к одиночным выбросам.

Вычисление Q-статистики для распределения записей аудита.

$$f_{m,k} = \frac{1}{N_k} \sum_{j=1}^{n} \left(W_{m,j} 2^{-b(k-j)} \right)$$

$$N_n = \sum_{j=1}^{k} W_j 2^{-b(n-j)}$$

$$Q_n = N_n \sum_{m=1}^{M} \left[\left(g_{m,n} - f_m \right)^2 / f_m \right]$$

Значения для краткосрочного профиля.

$$g_{m,n} = \frac{1}{N_r}\sum_{j=1}^{n}\left[\mathrm{I}(j,m)2^{-r(n-j)}\right] = 2^{-r}\,g_{m,n-1} + \frac{\mathrm{I}(m,n)}{N_r}$$

$$N_r = \sum_{j=1}^{n} 2^{-b(r-j)}$$