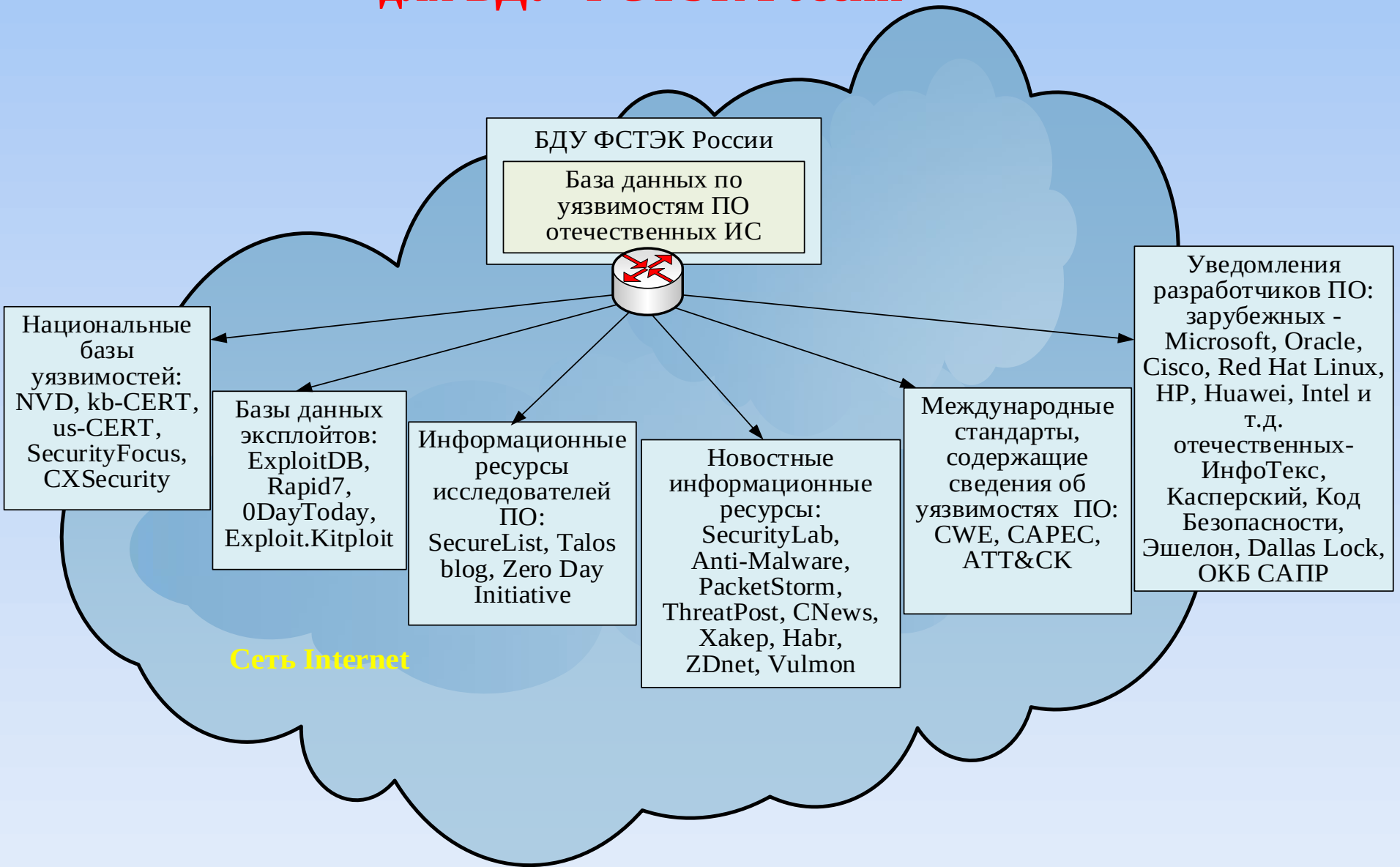
XXXI научно-практическая конференция «Комплексная защита информации»
г. Москва, 6 – 7 октября 2026 г.

Язов Ю.К., Тарелкин М.А.

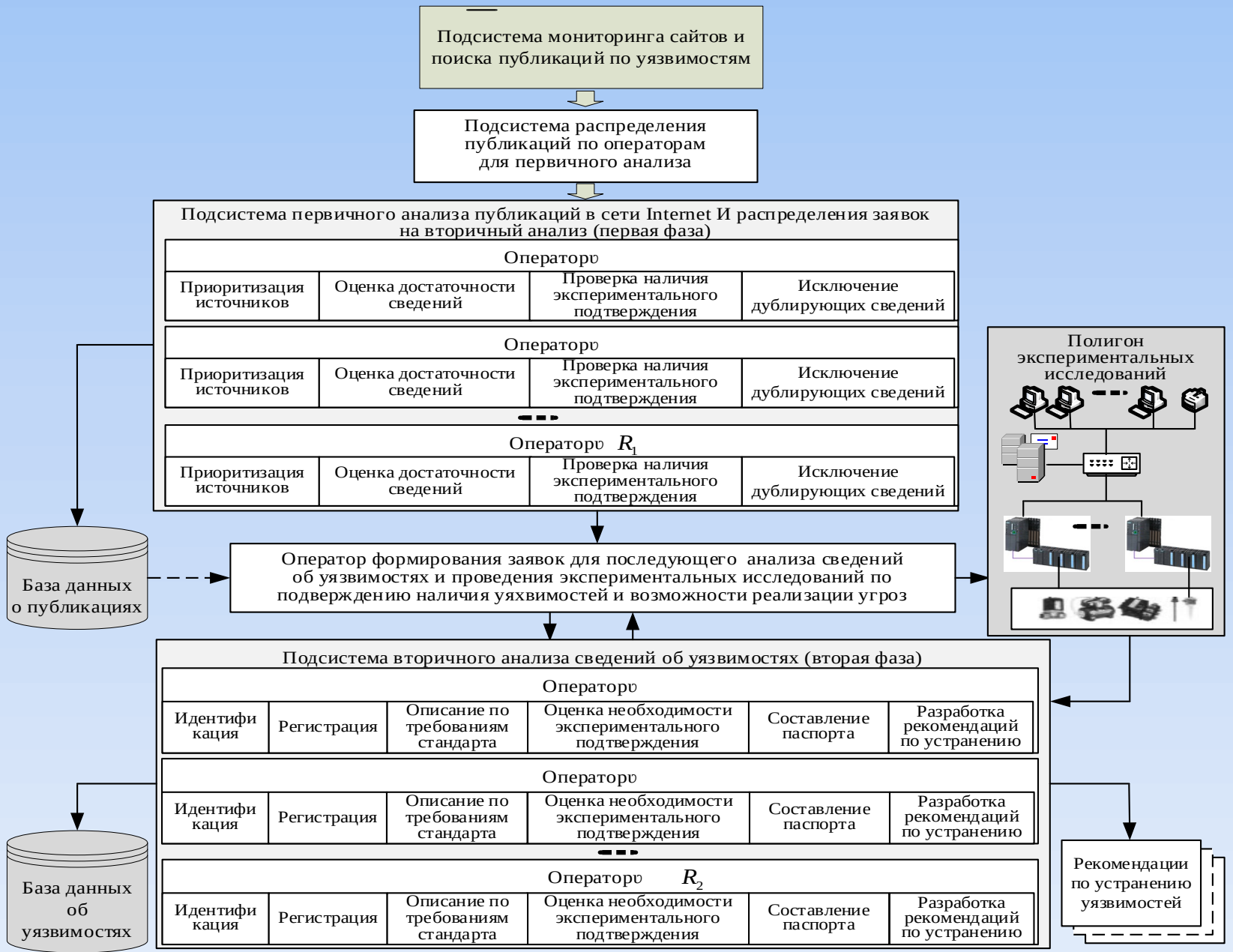
МАТЕМАТИЧЕСКИЕ МОДЕЛИ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ АНАЛИЗА УЯЗВИМОСТЕЙ С ИСПОЛЬЗОВАНИЕМ АППАРАТА ТЕОРИИ СТОХАСТИЧЕСКИХ СИСТЕМ МАССОВОГО ОБСЛУЖИВАНИЯ

Докладчик:
доктор техн. наук, проф. Язов Юрий Константинович,
ФАУ «ГНИИИ ПТЗИ ФСТЭК России», г. Воронеж

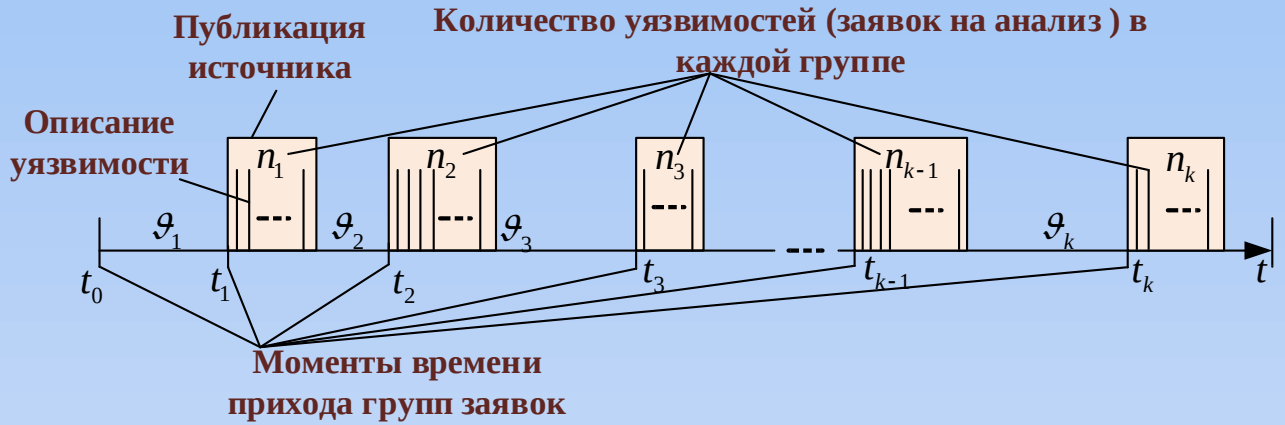
Источники сведений об уязвимостях для БДУ ФСТЭК России



Многоканальная СМО для анализа уязвимостей

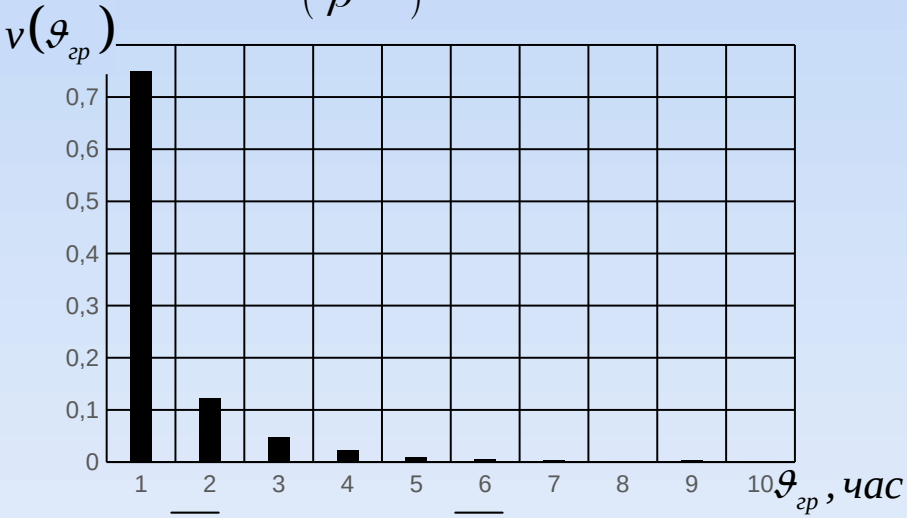


Неординарные потоки публикаций сведений об уязвимостях

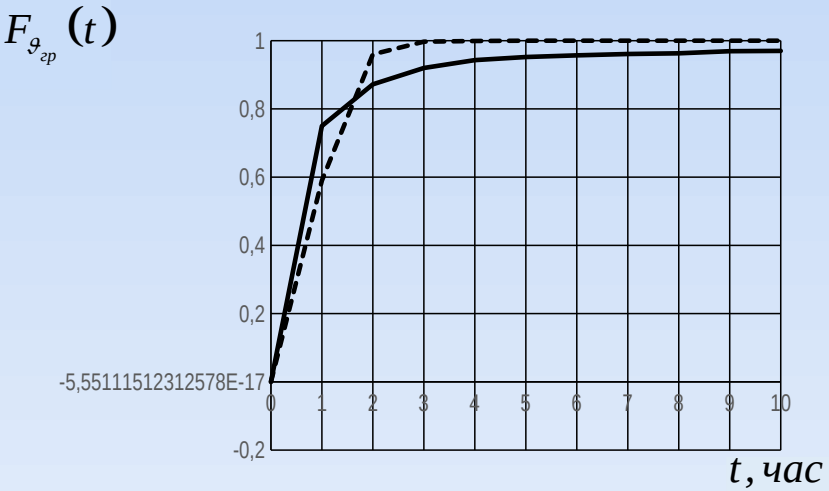


$$F_{\vartheta_{гр}}(t) = \int_0^t \frac{1}{\beta^{\alpha} \cdot (\alpha - 1)!} \cdot x^{\alpha-1} \cdot exp\left(-\frac{x}{\beta}\right) dx = \gamma\left(\frac{t}{\beta}, \alpha\right) \qquad (4.1)$$

$\gamma\left(\frac{t}{\beta}, \alpha\right)$ - неполная гамма - функция; $\beta = 0{,}27 час, \alpha = 3.9, \overline{\vartheta_{гр}} = \alpha \cdot \beta = 1.05 часа$

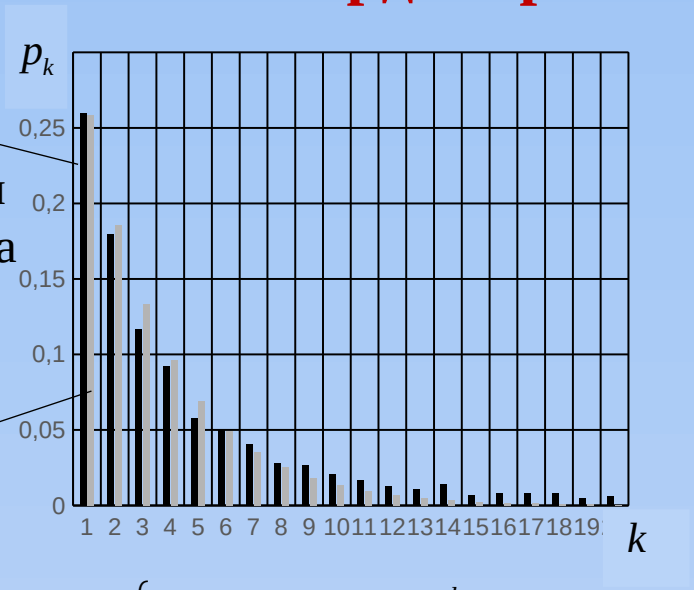


$\overline{\vartheta_{гр}} \approx 1 час, \sigma_{\vartheta} \approx \overline{\vartheta_{гр}}$



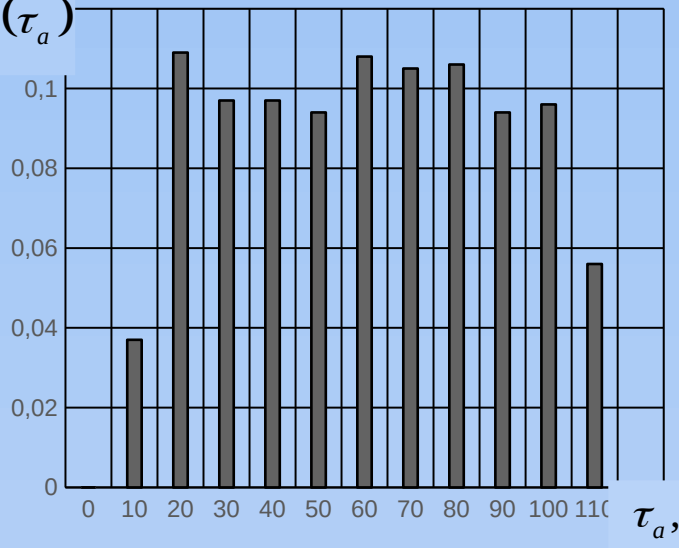
Статистика по количеству описаний уязвимостей в группе неординарного потока публикаций

По результатам мониторинга



По результатам расчета по формуле (5.1)

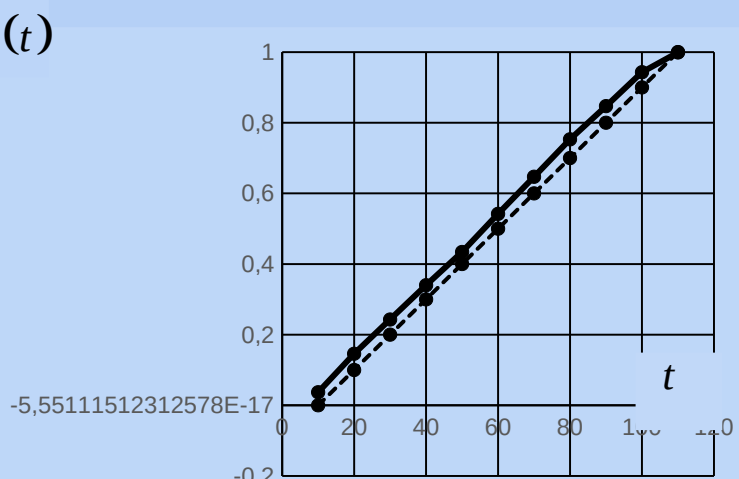
$$\begin{cases} p_k \approx m_{уяз} \cdot e^{-m_{уяз} k} \\ m_{уяз} = \sigma_{уяз} \approx 4.5 \end{cases} \qquad (5.1)$$



τ_a - время анализа описания одной уязвимости

$$F_\tau(t) = \frac{t - \tau_a^{(min)}}{\tau_a^{(max)} - \tau_a^{(min)}}, t \in \left[\tau_a^{(min)}, \tau_a^{(max)}\right] \qquad (5.2)$$

$\overline{\tau_a} = 58$мин, $\sigma_a = 29$мин



Математическая модель динамики первичного анализа уязвимостей

Система уравнений Колмогорова для неординарного потока публикаций

$$P_0'(t) = -\lambda_{gr} \cdot P_0(t) + \mu_{gr} \cdot P_1(t); \qquad (6.1)$$

$$P_j'(t) = -\left(\lambda_{gr} + \mu_{gr} \cdot min(j,r)\right) \cdot P_{j-1}(t) + min(j+1,r) \cdot \mu_{gr} \cdot P_j(t) + \lambda_{gr} \cdot \sum_{k=1}^{j-1} p_k \cdot P_{j-k}(t), j \geq 1;$$

система уравнений Колмогорова для стационарного режима

$$\begin{cases} 0 = -\lambda_{гр} \cdot \pi_0 + \mu_a \cdot \pi_1; \\ 0 = -\left(\lambda_{гр} + \mu_a \cdot min(j,r)\right) \cdot \pi_{j-1} + min(j+1,r) \cdot \mu_a \cdot \pi_j + \lambda_{гр} \cdot \sum_{k=1}^{j-1} p_k \cdot \pi_{j-1-k}(t), j \geq 1, \end{cases} \qquad (6.2)$$

где π_j вероятность того, что r- канальная СМО в стационарном режиме находится в состоянии j, при этом $\sum_j \pi_j = 1;$

$\lambda_{гр} = \frac{1}{\vartheta_{гр}}$ - интенсивность потока публикаций (групп описаний уязвимостей);

$\mu_a = \frac{1}{\tau_a}$ - интенсивность анализа каждого описания уязвимости.

Математическая модель динамики первичного анализа уязвимостей (продолжение)

Решение системы уравнений Колмогорова осуществляется с использованием аппарата производящих функций: $\Phi(z)=\sum_{j=0}^{\infty} z^j \pi_j,\ \Phi^{(j)}(0)=j!\pi_j.$ (7.1)

В результате получена формулы для расчета производящей функции и вероятностей π_j

$$\Phi(z)=\frac{\mu\left(1-\frac{1}{z}\right)\sum_{j=0}^{r-1}(r-j)z^j\pi_j+\sum_{j=0}^{\infty}z^j\sum_{i=0}^{j-1}p_k\cdot\pi_{j-1-i}}{\lambda+\mu r\left(1-\frac{1}{z}\right)} \quad (7.2)$$

$$\begin{cases}
\pi_0=1-m_{уяз}\frac{\lambda_{гр}}{\mu_a};\ \pi_1=\pi_0\frac{\lambda_{гр}}{\mu_a},r=1;\\
\pi_j=\left[\frac{\lambda_{гр}+\mu_a(j-1)}{\mu_a j}\right]\pi_{j-1}+\frac{\lambda_{гр}}{\mu_a j}\cdot\sum_{k=1}^{j-1}p_k\cdot\pi_{j-1-k},\ j<r-1,r\geq 2;\\
\pi_j=\frac{\lambda_{гр}+r\mu_a}{\mu_a(r-1)}\pi_{j-1}-\frac{\lambda_{гр}}{\mu_a(r-1)}\sum_{k=1}^{j-1}p_k\cdot\pi_{j-1-k},\ j=r-1,r\geq 2;\\
\pi_j=\frac{\lambda_{гр}-(r-1)\mu_a}{r\mu_a}\pi_{j-1}-\frac{\lambda_{гр}}{r\mu}\sum_{k=1}^{j-1}p_k\cdot\pi_{j-1-k},\ j=r,\ r\geq 2;\\
\pi_j=\left(\frac{\lambda_{гр}+r\mu_a}{r\mu_a}\right)\pi_{j-1}-\frac{\lambda_{гр}}{r\mu_a}\sum_{k=1}^{j-1}p_k\cdot\pi_{j-1-k},\ j>r,\ r\geq 2;
\end{cases} \quad (7.3)$$

Математическая модель динамики вторичного анализа уязвимостей

Система уравнений Колмогорова

$$\begin{cases} 0 = -(\lambda + \mu \cdot j)\cdot \pi_j + (j+1)\mu \cdot \pi_{j+1} + \lambda \pi_{j-k}, j \le r-1; \\ 0 = -(\lambda + \mu \cdot r)\cdot \pi_j + r\mu \cdot \pi_{j+1} + \lambda \pi_{j-k}, \; j \ge r. \end{cases} \quad (8.1)$$

Производящая функция

$$\Phi(z) = \left[\mu \sum_{j=0}^{r-1} (r - j) z^j \pi_j \right] \Big/ \left[\mu r - \frac{\lambda z (1 - z^k)}{\mu r (1 - z)} \right]. \quad (8.2)$$

Вероятность π_j пребывания СМО в состоянии j

$$\pi_0 = 1 - k\frac{\lambda_{гр}}{\mu_a} \text{ и } \pi_1 = \pi_0 \frac{\lambda_{гр}}{\mu_a}, \; r = 1; \quad (8.3)$$

$k < n$

$$\begin{cases} \pi_n = \left(\frac{\lambda}{\mu r} + 1 \right) \pi_{n-1}, n > r; \\ \pi_n = \left(\frac{\lambda}{\mu r} + 1 - \frac{1}{r} \right) \pi_{n-1} - \frac{\lambda (k+1)! (n-k-1)!}{\mu r n!} \pi_{n-k-1}, n = r; \\ \pi_n = \left[\frac{\lambda}{\mu n} + 1 - \frac{1}{n} \right] \pi_{n-1} + \frac{\lambda (k+1)! (n-k-1)!}{n \cdot \mu \cdot n!} \pi_{n-k-1}, n < r. \end{cases}$$

$k \ge n$

$$\begin{cases} \pi_n = \left(\frac{\lambda}{\mu r} + 1 \right) \pi_{n-1}, n > r; \\ \pi_n = \left[\frac{\lambda + \mu (r-1)}{\mu r} \right] \pi_{n-1}, n = r; \\ \pi_n = \left(\frac{\lambda}{\mu n} + \frac{r}{n} \right) \pi_{n-1}, n < r; \end{cases} \quad (8.4)$$

Выводы

1. Опыт эксплуатации БДУ ФСТЭК России показал, острую необходимость повышения производительности системы анализа уязвимостей, сведений о которых публикуются в Internet. Однако отсутствие до сих пор статистические характеристики трафика публикаций, сдерживало обоснование путей совершенствования такой системы. В данной докладе впервые показано, что поток публикаций является неординарным, и приведены эти характеристики, положенные в основу разработанных аналитических моделей процесса анализа уязвимостей на основе аппарата теории стохастических систем массового обслуживания.

2. Функционирующая сегодня в БДУ ФСТЭК России система анализа публикаций является двухфазной СМО, когда на первой фазе рассматриваются группы публикаций со случайным количеством уязвимостей в каждой группе, а на второй – группы описаний самих уязвимостей с детерминированным количеством заявок на вторичный анализ. Разработанные аналитические модели двухфазного процесса анализа уязвимостей ПО ИС позволяют рассчитывать показатели качества функционирования таких СМО с учетом реальных статистических характеристик потоков публикаций сведений об уязвимостях в сети Internet. Модели могут быть использованы как России, так и в Беларуси, в организациях, при оценке эффективности функционирования систем анализа и обосновании на количественной основе требований к таким системам в интересах повышения их производительности в условиях нарастающего объема трафика публикаций

Спасибо за внимание!

Язов Юрий Константинович