## 4.3. Эффективность системы информационной безопасности

Под внешним воздействием на безопасность АИС будем понимать комплекс действий, вызываемых программными злоупотреблениями [172]. При моделировании внешних воздействий достаточно сложно, по нашему мнению, однозначно формализовать процессы влияния программных злоупотреблений, поскольку они значительно отличаются внутренней организацией, методами распространения, экономическими следствиями и т.д.

Введем следующие переменные для описания процессов воздействия программных злоупотреблений:

$d$ - оценка пораженных объектов АИС (файлов, программ, узлов и т.д.);

$\beta$ - оценка непораженных объектов;

$t$ - временной интервал;

$N$ - общее количество объектов в АИС.

В соответствии с [204] используем переменную $\rho$, которая характеризует "эпидемиологическую границу" $\left(\rho=\frac{s}{\beta}=1\right)$. В случае, если $\beta>d$ и $\rho<1$, состояние АИС можно охарактеризовать как F1 и вирусная эпидемия развивается с вероятностью $1-\rho$. В данном случае количество пораженных объектов возрастает экспоненциально ( $\gg e^{(\beta-d)t}$ ) и возможное насыщение определяется как $N(1-\rho)$. Для случая, когда $\beta<d$ и $\rho>1$, состоние системы описывается как F2 и характеризуется потерей работоспособности АИС.

Состояния F1 и F2 характеризуют два полярных состояния АИС. Первое (F1), несмотря на наличие активных программных злоупотреблений, сохраняет допустимую устойчивость и равновесие, обеспечивает работоспособное состояние. Второе (F2), характеризуется состоянием с характеристиками ниже допустимых и потерей работоспособности. Использование $\rho$ для характеристики состояния АИС имеет вероятностный характер и зависит от множества факторов.

Уровень "эпидемиологической границы" ( $\rho$ ) для различных АИС может существенно отличаться. Это зависит, во-первых, от топологии, которая напрямую корреспондируется со скоростью распространения программных злоупотреблений (уменьшение количества узлов системы приводит к снижению вероятности развития "вирусной эпидемии"). Другим важным фактором является совокупность платформ, используемых в АИС. Известно, что большинство программных злоупотреблений разрабатываются и реализуются для определенных платформ. При переходе с одной платформы на другую программное злоупотребление может просто не работать. Тип системы (гомогенная, распределенная или локальная), также оказывает влияние на организацию доступа прикладных процессов (в том числе и программных злоупотреблений) к информационным, вычислительным и коммуникационным ресурсам.

Во-вторых, существенное влияние оказывает организация и тип самого программного злоупотребления (например, если это компьютерный вирус, то весьма важным являются его основные характеристики - резидентный, активный и т.п.).

В-третьих, наличие антивирусного программного обеспечения и реализация контрольных операций существенно снижают (но не устраняют) вероятность развития эпидемии и перехода к состоянию F2.

Последнее обстоятельство является существенным, поскольку антивирусное программное обеспечение и контрольные операции сдерживают развитие "вирусной инфекции" за счет вакцинирования пораженных и непораженных объектов. Если через V обозначить деятельность вирусного механизма, а через K - антивирусного, то соответственно:

$\beta_k$ - оценка непораженных и вакцинированных объектов;

$\beta_v$ - оценка непораженных, но потенциально подверженных поражению;

$d_k$ - оценка пораженных объектов, подвергнутых "лечению" и вакцинированию;

$d_v$ - оценка пораженных объектов.

Для оценки состояния АИС во времени (при одновременном функционировании программных злоупотреблений и антивирусного программного обеспечения) возможно использование следующих нелинейных дифференциальных уравнений:

$$\frac{dv}{dt} = \beta_v(1 - v - k) - d_k - \beta_k vk \qquad (4.45)$$

$$\frac{dv}{dt} = \beta_k vk - d_k k + d_v$$

Следует отметить, что формула (4.45) может быть использована для определения объемов *v(t)* и *k(t)*, соответственно.

Предположим, что после некоторого периода времени число пораженных объектов составит *n* и состояние F2 можно представить как $nd$ , а деятельность по уничтожению и вакцинированию объектов как $n(1-n/n)\rho$ , при общем количестве объектов АИС равном *N*.

Вероятность перехода от n пораженных объектов к *n+1* можно рассчитать следующим образом:

$$P_{n \to n+1} = \frac{(1 - n/N)}{(1 - n/N) + \rho} \approx \frac{1}{1 + \rho} \qquad \text{при } n < N \qquad (4.46)$$

Соответственно, вероятность поражения составит:

$$P(n) = (1 - P_{n \to n+1}) \prod_{i=1}^{i=n-1} P_{i \to i+1} \approx \frac{\rho}{(1+\rho)^n} ,$$

(4.47)

и соответственно математическое ожидание

$$m = \sum_n nP(n) \approx 1 + \frac{1}{\rho} . \qquad (4.48)$$

Предположим, что в АИС существует *n* инфицированных объектов за время *t*. Скорость перехода от *n* к *n+1* можно определить следующим образом:

$$R_{n \to n+1} = \beta n(1 - \frac{n}{N}) , \qquad (4.49)$$

а скорость открытия и уничтожения программного злоупотребления как $R_{n \to 0} = dn$ . Вероятность развития вирусного механизма (в том случае, если в основе программного злоупотребления использован вирусный

механизм), которая описывается как *p(n,t)* для *n>1*, определяется следующим образом:

$$\frac{dp(n,t)}{dt} = - p(n,t)[R_{n\to n+1} + R_{n\to 0}] + \rho(n-1,t) R_{n-1\to n} . \quad (4.50)$$

Соответственно, случай *p(0,t)* может быть представлен с помощью следующего выражения:

$$\frac{dp(o,t)}{dt} = \sum_{n^3 1} p(n,t) dn , \quad (4.51)$$

или в нормализованном виде

$$P(o,t) = 1 - \sum_{n^3 1} p(n,t) . \quad (4.52)$$

Задавая первоначальные условия, что *p(1,t)=1; p(n,t)=0* и *n=1*, получаем:

$$\frac{dp(1,t)}{dt} = - p(1,t)[\beta, d] . \quad (4.53)$$

Подставив значение *p(1,0)=1*, получаем

$$p(1,t) = e^{-(\beta+d)t} \quad (4.54)$$

Соответственно, для аналогичного случая p(2,t) имеем:

$$\frac{dp(2,t)}{dt} = - p(2,t)[2(\beta+d) + \beta p(1,t)] . \quad (4.55)$$

При исходном значении *p(2,0)=0* получаем следующее уравнение:

$$p(2,t) = \int_0^t e^{2(\beta+d)(t_1-t)} \beta p(1,t_1) dt_1 = \frac{\beta}{\beta+d}\left[1 - e^{-(\beta+d)t}\right] e^{-(\beta+d)t} \quad (4.56)$$

В общем случае, решение для *p(n,t)* может быть найдено через *p(n-1,t)*:

$$p(n,t) = \int_0^t e^{n(\beta+d)(t_1-t)} (n-1) \beta p(n-1,t_1) dt_1 = \left[\frac{\beta}{\beta+d}\left[1 - e^{-(\beta+d)t}\right]\right]^{n-1} e^{-(\beta+d)t} \quad (4.57)$$

Подставив *p(0,t)* в формулу (4.57), уравнение (4.52) решается следующим образом:

$$P(0,t) = \frac{d(1 - e^{-(\beta+d)t})}{d + \beta e^{-(\beta+d)t}} \quad (4.58)$$

Таким образом, функция *p(0,t)* монотонно возрастает от *0 (t= 0)* к *1* (при $t \to ¥$ ).

Для оценки развития вирусного механизма используем отрезок времени *t'*, который характеризуется бесконечно малым интервалом

$t<t'<t+Dt$ и описывается как $p(n,t)dnDt$. Заменяя $(1-e^{-(\beta+d)t})\to x$, можно определить вероятность поражения как

$$P(n)=\int_0^{\infty} dtp(n,t)n=\frac{\rho}{(1+\rho)^n}n\int_0^1 dxx^{n-1}=\frac{\rho}{(1+\rho)^n}, \quad (4.59)$$

что полностью согласуется с формулой (4.47).

Продолжительность инциндента $Q(n,t)$ характеризует время распространения $\int_0^{\infty} dtQ(n,t)=1$ для любых $n$:

$$Q(n,t)=\beta n(1+\rho)^n p(n,t)=(\beta+d)n[1-e^{-(\beta+d)}]^{n-1}e^{-(\beta+d)t}$$

(4.60)

Для поиска средней продолжительности $Q(n)$ размером $n$ решается следующее уравнение:

$$Q(n)=\int_0^{\infty} dttQ(n,t)=-\frac{n}{\beta+d}\int_0^1 dxx^{n-1}\ln(1-x)=\frac{1}{\beta+d}\sum_{j=1}\frac{1}{j}$$

(4.61)

Для достаточно большого n формула (4.61) приближенно равна:

$$Q(n)\approx\frac{1}{\beta+d}\left[\ln(n)+g+\frac{1}{2n}\right] \quad (4.62)$$

где $g$ =0,57721 - константа Эйлера.

При оценке надежности СИБ необходимо принимать во внимание обстоятельство, связанное с изменением среды функционирования АИС и допусками отдельных элементов. По аналогии с техническими системами и расчетом надежности их элементов используем показатель "дрейфа", характеризующий процесс изменения характеристик элементов СИБ (старение, деградация и др.). В отличие от [183,184], где оптимизация дрейфа надежности технических систем ставится в зависимость от воздействия окружающей среды (температура, влажность и др.), рассмотрим параметрические пределы надежности системы безопасности.

Для данного случая надежность определяется как вероятность безотказной работы СИБ в течение заданного интервала времени и условий функционирования. Дрейф системы безопасности - ограничение пределов надежности, а дрейф надежности - вероятность того, что система безопасности будет работать безотказно в течение

заданного времени, если причиной отказа является только дрейф параметров элементов СИБ.

Элементы СИБ являются субъектами допусков, которые характеризуют:

- нормальные (стандартные) условия функционирования АИС;

- катастрофические отказы, вызванные воздействием внешних условий (например, несанкционированными действиями пользователей, которые привели к потере работоспособности, отказу в предоставлении ресурсов, потере доверия пользователей и др.).

Параметрический предел надежности элементов СИБ (Y(x)) опишем с использованием следующих переменных:

$e$ - вектор фактических значений параметров ( $e \hat{I} R^n$ );

$x$ - вектор номинальных значений параметров ( $x \hat{I} R^n$ );

$x * Q$ - вектор нормализованных значений параметров ( $x * Q \hat{I} R^n$ ), который определяется как $Q_t = (e_t * x_t) / s_t$ ;

$\beta$ - вероятность плотности распределения дрейфа (старение, деградация элементов СИБ);

$t$- временной интервал, $t = \overline{o, T}$ ;

Параметрический предел рассчитывается как

$$\max_{x \hat{I} R^n} \{Y(x)\} = \int_{R^n} Æ(e) f_e(x, \beta, e) = \int_{R^n} Æ\{e(x, \beta, Q) dQ\} \qquad (4.63)$$

где $f_e(x, \beta, e)$ - вероятность плотности распределения функции $e \beta \hat{I} R^n$, то есть вектор параметров, характеризующих вероятность плотности распределения функции $f_e(.)$ .

Формулу (4.63) можно записать следующим образом:

$$Y(x) = E_e[Æ(e)] = E_Q[Æ\{e(x, \beta, Q)\}] \qquad (4.64)$$

Параметры $x$ и $\beta$ являются функциями, которые характеризуют условия функционирования СИБ во времени, и если они известны, то можно определить:

$$Y(x, c, t) = \int_{R^n} Æ(e(x, c, t, Q)) f_Q(Q) dQ \qquad (4.65)$$

где $c$- внешние воздействия на СИБ.

Несмещенные оценки могут быть получены как среднее из (4.65):

$$Y(x,c,t)=\frac{1}{N}\sum_{i=1}^{N} Æ(e(x,c,t,Q))=\frac{N_i(t)}{N}\ , \qquad (4.66)$$

где $N_i$ - количество элементов СИБ, сохранивших работоспособность в момент $t$.

Для фиксированных условий влияния внешней среды ($c=Const$), максимизация среднего времени безотказной работы определится следующим образом:

$$\max_x\{M(x,c)\}=\int_0^{¥} RS_d(x,c,t)\,dt\ , \qquad (4.67)$$

где $RS_d$ - условная вероятность безотказной работы элементов СИБ.

Среднее время наработки на отказ рассчитывается следующим образом:

$$M_0=\int_0^{¥} RS_d(t)\,d(t)=\frac{1}{Y(0)}\int_0^{¥} RS_d(t)\,d(t)=\frac{M}{Y(0)}\ ,$$

(4.68)

откуда $M=Y(0)M_0$ . (4.69)

Оценка дрейфа параметров СИБ можно поставить в соответствие изменению внешних условий (среды функционирования) и выразить с помощью вектора случайных параметров. Параметр $\overline{MT}$ , означающий новые значения среднего времени наработки на отказ, определяется как:

$$\overline{MT}(x)=\frac{1}{M}\sum_{m=1} f(c^m)MT(x,c^n)$$

(4.70)

где $MT$ - множество векторов, характеризующих внешние условия воздействия на СИБ;

$f(c^m)$ - весовая функция, характеризующая важность специфических комбинаций внешних условий воздействия.

При проектировании структуры и размещения элементов СИБ предусматривается избыточность элементов, обеспечивающая запас производительности и снижение возможных потерь от внешних воздействий. Предположим, что все элементы СИБ действуют независимо, с постоянной интенсивностью отказов и избыточность СИБ описывается n элементами, из

которых $k$ необходимы для поддержания работоспособности. Рассмотрим стоимость СИБ и средние потери, вызванные внешними воздействиями.

Средние потери от внешних воздействий могут определяться как

$$L_{ср}=rc^1 P\{x<k\}=rc^2 f(k-1;p,n) \qquad (4.71)$$

где $r$- надежность подсистемы;

$c^1$- стоимость отказа подсистемы.

Общая стоимость подсистемы,включая средние потери от внешних воздействий, равна

$$C^0{}_{общ}=nc^4+rc^1 f(k-1;p,n) \qquad (4.72)$$

где $c^4$ - стоимость одного элемента СИБ.

В свою очередь, полная стоимость подсистемы определяется как

$$C^0{}_{п}=nc^3 g(k)/k+rc^1 f(k-1;p,n)\ , \qquad (4.73)$$

где $c^3$- стоимость одноэлементной подсистемы;

$c^3g(k)$- общая стоимость подсистемы из $k$ элементов.

При воздействии внешней среды на АИС предполагается, что СИБ обладает определенным запасом "прочности" и в состоянии противостоять основным типам программных злоупотреблений. Введем дополнительные переменные для характеристики потерь:

$V$ - относительное состояние СИБ, обеспечивающее работоспособность АИС ($v=x/k$, где $x$ - число отказавших систем);

$V_{min}$- минимальный (пороговый) уровень, обеспечивающий работоспоосбность СИБ;

$c^2$- потери на уровне $v$.

Функция потерь на уровне $v$ $(Lv)$ может быть определена следующим образом

$$L(v)=c^2/(1-V_{\min})(1-v) \qquad 0<V_{\min}<1 \qquad (4.74)$$

Общая стоимость с учетом потерь из-за частичного отказа равна

$$C_o^0=nc^3 g(k)/k+rc^1\sum_{x=0}^{x<kV_{min}} f(x;p,n)+r\sum_{x^3kV_{min}}^{k-1} f(x;p,n)[(c^2¿1-V_{\min})-(c^2¿1-V_{\min})x/k\,]$$

(4.75)

Для случая, когда стоимость отказа подсистемы равна потерям на уровне $v(c^1 = c^2)$ и АИС сохранила работоспособность в течении интервала времени $t$, то вероятность безотказной работы равна $e(-\lambda t)$, где $\lambda$ - интенсивность отказов.

Задавая время наработки на отказ как величину $T$, определим

$$f(t|x)=L(t,x)/\int_0^t L(t|x)\,dt \qquad 0<t<T$$

(4.76)

где

$$L(t|x)=\frac{u!}{x!(u-x-1)!}\left[e(-\lambda t)^x \lambda e(-\lambda t)(1-e(-\lambda t))\right]^{u-x-1}$$

и

$$f(x,t)=f(t|x)g(x)$$

$$g(x)=f(x;e(-\lambda t),n)$$

В общем случае с учетом функции потерь $L(v,t)$ стоимость отказа определяется с использованием следующего уравнения:

$$C_o^0=nc^3 g(k)/k+r\sum_{x=0}^{n}\int_0^T L(x/k,t)f(x,t)\,dt\ , \qquad (4.77)$$

где

$$L(x/k,t)=d(x,k)\sum c^2/(1-V_{\min})t\ .$$