

Модель анализа последствий воздействия внутренних угроз информационной безопасности на основе Марковского случайного процесса

Информационная безопасность является неотъемлемой частью эффективного функционирования предприятий, учреждений и организаций различного масштаба и рода деятельности. На всех стадиях информационного процесса ведущая роль принадлежит человеку - носителю, пользователю информации. От того, как будут учтены в информационных процессах интересы, свойства личности, зависит эффективность использования информации.

Профессиональная деятельность персонала в информационных системах и сетях, разумеется, регламентирована нормами и правилами выполнения функциональных задач. Любые нарушения, отклонения от нормативной деятельности можно трактовать либо как умышленные действия, либо как непреднамеренные, зачастую случайные ошибки. Это два главных класса угроз безопасности. И те, и другие могут приводить к непоправимым последствиям. Чем более критичен элемент информационной инфраструктуры для жизнедеятельности общества и государства, тем более существенен ущерб, наносимый этими нарушениями. Возможность нарушений делает профессиональную деятельность персонала одним из самых уязвимых звеньев в человеко-машинных системах обработки и передачи информации.

Указанная проблема подтверждается анализом имеющейся статистической информации о влиянии внутренних угроз на безопасность КИ. Исследования показывают, что в настоящее время внутренние угрозы уже превалируют над внешними.

Структурно взаимодействие человека-оператора и АИС можно отобразить следующим образом:



Как видно из представленной схемы, конечной целью исследования является анализ защищенности ИОР, циркулирующей в АИС. Учитывая особенности деятельности человека-оператора необходимо рассмотреть такие аспекты безопасности, которые опосредованно, через характеристики надежности оператора воздействуют на надежность системы ЗИ АИС. В свою очередь на характеристики надежности системы ЗИ и оператора оказывает влияние степень функциональной согласованности технических и эргономических свойств АИС и системы ЗИ с набором характеристик человека-оператора, оказывающих влияние на надежность его функционирования в качестве подсистемы ЗИ.

Методика оценки построена на математическом аппарате структурно-алгоритмического описания объектов, Марковского случайного процесса с дискретным параметром.

Итак, представим, что деятельность человека-оператора представляет собой некоторую последовательность элементарных операций, следующих друг за другом, целесообразно для построения модели использовать структурно-алгоритмическое моделирование.

Итак, пусть в терминах, используемых при алгоритмическом описании объектов управления определены l задач и m режимов работы сотрудника, причем в силу некоторой энтропии ситуации решение i -ой задачи ($i=1, 2, \dots, l$) в g -ом состоянии ($g=1, 2, \dots, m$) возможно n способами, так что j -тый способ

($j=1, 2, \dots, n$) выбирается сотрудником смотря по обстоятельствам, либо из числа заученных в прошлом, либо благодаря эвристической деятельности. Иначе говоря, i -ая задача в $г$ -ом состоянии решается сотрудником по вероятностному алгоритму, каждая i -ая реализация которого осуществляется с некоторой частотой $f_{г,i,j}$, определенной на полной группе n несовместных реализаций, и представляется собой детерминированную последовательность конечного числа некоторых элементарных действий)

Тогда, кодируя операции j -ой реализации i -го алгоритма в некотором алфавите символов, можно построить ориентированный граф (орграф), вершины которого есть символы операций, а дуги между вершинами обозначают переходы между операциями. Такому орграфу изоморфна матрица смежности. Это квадратная матрица $A_{г,i,j}$, число строк и столбцов которой на единицу больше количества различных операций j -ой реализации, а элементы которой $a_{p,q}$ характеризуют частоту следования действия (или размышления) q непосредственно за действием (размышлением) p ($a_{p,q}=0, 1, 2, \dots$).

Пусть для i -ой задачи в $г$ -ом состоянии определены все n реализаций, т.е. заданы матрицы $A_{г,i,j}$ и

частоты $f_{г,i,j}$. Тогда они обобщаются в матрицу $B_{г,i}$, описывающую вероятностный алгоритм решения i -ой задачи в $г$ -ом состоянии:

$$B_{г,i} = \bigcirc_{j=1}^n A_{г,i,j} f_{г,i,j}, \quad (1)$$

где $A_{г,i,j}$ – матрица смежности;

$f_{г,i,j}$ – частота реализации алгоритма.

Операция обобщения ($\bigcirc_{j=1}^n$) осуществляется следующим образом:

1. Из строк матриц $A_{г,i,j}$ выбираются все различные символы операций, которые образуют упорядоченные строки столбцы основы матрицы $B_{г,i}^0$;

2. В каждую $A_{г,i,j}$ добавляют строки и столбцы (с нулевыми элементами), символы которых входят в $B_{г,i}^0$, но отсутствовали в $A_{г,i,j}$;

3. Дополненную таким образом $A_{г,i,j}$ перестановкой рядов приводят к одной и той же упорядоченной форме $B_{г,i}^0$;

4. Поэлементно суммируют все $A_{г,i,j}$ в матрицу $B_{г,i}$, предварительно взвешивая их частотами $f_{г,i,j}$

Аналогично (1) получают:

а) матрица C_r для $г$ -го состояния работы:

$$C_r = \bigcirc_{i=1}^l B_{г,i} f_{г,i} \quad (2)$$

где $B_{г,i}$ – матрица решения i -ой задачи в $г$ -ом состоянии;

$f_{г,i}$ – частота появления i -ой задачи в $г$ -ом состояниях;

б) матрица D для работы сотрудника при всех m состояниях

$$D = \bigcirc_{r=1}^m C_r f_r = \bigcirc_{r=1}^m \left[\bigcirc_{i=1}^l \left(\bigcirc_{j=1}^n A_{г,i,j} f_{г,i,j} \right) f_{г,i} \right] f_r, \quad (3)$$

где $f_{г,i}$ – частота появления i -ой задачи в $г$ -ом состоянии;

f_r – частота r -го режима в деятельности сотрудника.

Данная структурно-алгоритмическая модель деятельности сотрудника представляет собой таким образом, совокупность матриц A_{rij} , B_{ri} , C_r и (или) изоморфных им графов которые могут быть обобщены, согласно (3), в матрицу D , либо в граф, описывающий поведение сотрудника в целом.

Такой подход позволяет нам использовать Марковский случайный процесс с дискретным параметром для построения модели оценки влияния заданных характеристик на итоговый показатель безопасности. Итак, представим, что все переходы системы человек-АИС из состояния в состояние происходит под действием каких-либо потоков событий (возникновение угроз безопасности, появление факторов, способствующих снижению показателей надежности оператора). Если все потоки, протекающие в системе простейшие, то процесс будет Марковским.

Таким образом, если система S находится в каком-то состоянии S_i , из которого есть непосредственный переход в другое состояние S_j , то мы будем представлять так, что на систему, пока она находится в состоянии S_i , действует простейший поток событий, переводящий её в состояние S_j .

Обозначим P_{ij} вероятность событий, переводящих систему из состояния S_i в состояние S_j . Имея в своем распоряжении размеченный граф состояний системы легко построить математическую модель данного процесса.

Пусть система S имеет n различных состояний $S_1, S_2, \dots, S_n$. Вероятностью i -го состояния будет вероятность $p_i(t)$ того, что в момент времени t система будет находиться в состоянии S_i . Для любого момента сумма всех вероятностей состояний равна 1.

Если для каждого состояния системы известны вероятности перехода в любое другое состояние, то можно составить матрицу переходных вероятностей вида:

$$\|P_{ij}\| = \begin{vmatrix} P_{11} & P_{12} & \dots & P_{1j} & \dots & P_{1n} \\ P_{21} & P_{22} & \dots & P_{2j} & \dots & P_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ P_{i1} & P_{i2} & \dots & P_{ij} & \dots & P_{in} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ P_{n1} & P_{n2} & \dots & P_{nj} & \dots & P_{nn} \end{vmatrix}. \quad (3.1)$$

Из выражения (3.1) следует [84,91]:

диагональ матрицы соответствует вероятности задержки, т.е. система может задержаться в состояниях, при которых переход ее в следующее состояние не возможен;

вероятности P_{ij} являются условными вероятностями, смысл которых заключается в том, что после n -го шага система окажется в состоянии X_j , если до этого находилась в состоянии X_i ;

сумма вероятностей каждой строки матрицы (3.1) должна быть равна единице.

Пусть система в начальный момент (перед первым шагом) находится в состоянии X_n . Тогда, для начального момента ($n=0$) вероятности всех состояний равны нулю, кроме вероятности начального состояния $P_n(0)=1$.

После первого шага ($k=1$) система перейдет из состояния X_n в одно из состояний $X_1, X_2, \dots, X_n, \dots, X_k$ с вероятностями:

$$P_{n1}, P_{n2}, \dots, P_{nn}, \dots, P_{nk}.$$

Тогда n -я строка матрицы переходных вероятностей будет иметь вид:

$$P_1(1) = P_{n1}; P_2(1) = P_{n2}, \dots, P_n(1) = P_{nn}, \dots, P_k(1) = P_{nk}. \quad (3.2)$$

Вероятности состояний после второго шага определяется по формуле полной вероятности. Тогда:

$$P_i(2) = \sum_{j=1}^3 P_j(1) \cdot P_{ij}. \quad (3.3)$$

При этом должна выполняться гипотеза о том, что система после первого шага может быть в любом из возможных состояний.

Тогда, с учетом (3.3), по формуле полной вероятности матрица переходных вероятностей после k -го шага будет иметь вид:

$$P_i(k) = \sum_{j=1}^k P_j(k-1) P_{ji}, \quad (3.4)$$

где $i=1, 2, \dots, k$,

а вероятности перехода системы за k шагов с учетом (3.4) имеет вид:

$$P_{ij} = \sum_{n=1}^k P_{in} P_{nj}(k-1),$$

где $k \geq 2$.

Решение системы уравнений (3.4) позволяет определить любую вероятность $P_i(k)$ при известных начальных условиях: $P_1(0), P_2(0), \dots, P_k(0)$, т.е. при известном начальном состоянии системы. Исходными данными в этом случае служат вероятности перехода, которые могут задаваться стохастической матрицей (3.1).

Пусть на систему воздействует n независимых факторов. При этом очередной фактор воздействует на систему только после успешного парирования предыдущего. Процесс перехода системы из состояния в состояние происходит до тех пор, пока она не окажется в поглощающем состоянии, соответствующем реализации неблагоприятного исхода от воздействия фактора.

Примем следующие обозначения:

R_i и $\bar{R}_i$ ($\bar{R}_i = 1 - R_i$) – вероятности успешного и неуспешного парирования i -го фактора соответственно;

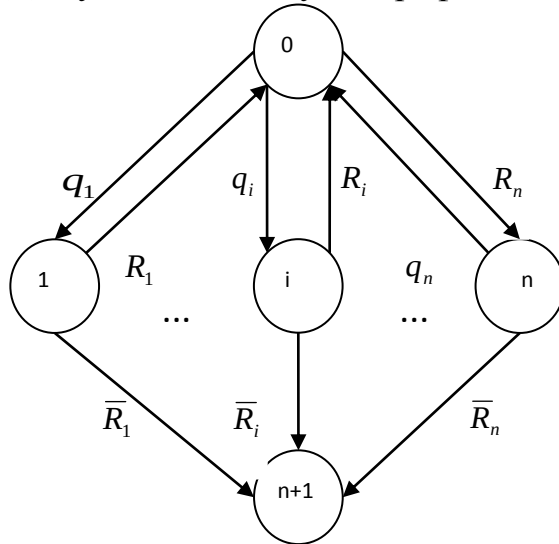
q_i – вероятность возникновения i -го фактора;

$0, 1, \dots, i, \dots, n, n+1$ – состояния, в которых может оказаться рассматриваемая система в результате воздействия n независимых факторов.

При этом состояние $n+1$ соответствует поглощающему состоянию.

Представим данную ситуацию в виде графа состояний системы.

Для указанного случая граф состояний представлен на рис. 3.2.



Как видно из рис. 3.2 при любом i -ом воздействии

оказаться с вероятностью R_i в исходном состоянии, что соответствует успешному парированию i -го фактора доступными методами и средствами.

В противном случае, она с вероятностью $\bar{R}_i = 1 - R_i$ может оказаться в поглощающем состоянии $n+1$, что соответствует реализации неблагоприятного исхода от воздействия i -го фактора.

В соответствии с рис. 3.2 матрица переходных вероятностей будет иметь следующий вид:

$$\|P_{ij}\| = \begin{vmatrix} q_{00} & q_1 & \dots & q_i & \dots & q_n & 0 \\ R_1 & q_{11} & \dots & 0 & \dots & 0 & \bar{R}_1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ R_n & 0 & \dots & 0 & \dots & q_{nn} & \bar{R}_n \\ 0 & 0 & \dots & 0 & \dots & 0 & q_{n+1,n+1} \end{vmatrix}. \quad (3.5)$$

Так как вероятность $q_{00} = 1 - q_\Sigma$ и соответствует вероятности невозникновения воздействия фактора в нулевом исходном состоянии, а вероятности $q_{11}, \dots, q_{ii}, \dots, q_{nn}, q_{n+1,n+1} = 0$, вследствие того, что в состояниях

$0, 1, \dots, i, \dots, n, n+1$ система по условию не может находиться (ранее было сказано, что из i -го состояния система с вероятностью R_i может перейти в исходное состояние и с вероятностью $\bar{R}_i = 1 - R_i$ – в поглощающее состояние, а вероятность $q_{n+1, n+1} = 1$, т.к. состояние $n+1$ поглощающее), тогда с учетом указанного матрица $\|P_{ij}\|$ примет следующий вид:

$$\|P_{ij}\| = \begin{vmatrix} 1 - q_{\Sigma} & q_1 & \dots & q_i & \dots & q_n & 0 \\ R_1 & 0 & \dots & 0 & \dots & 0 & \bar{R}_1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ R_i & 0 & \dots & 0 & \dots & 0 & \bar{R}_i \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ R_n & 0 & \dots & 0 & \dots & 0 & \bar{R}_n \\ 0 & 0 & \dots & 0 & \dots & 0 & 1 \end{vmatrix}. \quad (3.6)$$

Из матрицы (3.6) следует:

количество единиц в матрице по главной диагонали соответствует числу поглощающих состояний;

количество нулей в матрице соответствует числу невозможных переходов.

2.2.2.2 Определение вероятностей перехода системы в каждое возможное состояние.

Определим вероятность перехода системы в любое i -ое состояние для следующих исходных данных: $P_0(0) = 1$ и $P_1(0) = \dots = P_i(0) = \dots = P_n(0) = P_{n+1}(0) = 0$.

Тогда в соответствии с (3.2) после первого шага вероятности состояний будут иметь вид: $P_0(1) = 1 - q_{\Sigma}$, $P_{n+1}(0) = 0$, $P_1(1) = q_1$, ..., $P_i(1) = q_i$, ..., $P_n(1) = q_n$.

Вероятности состояний после второго шага:

$$\begin{aligned} P_0(2) &= P_0(1)P_{01} + P_1(1)P_{10} + \dots + P_i(1)P_{i0} + \dots + P_n(1)P_{n0} + P_{n+1}(1)P_{(n+1),0} = \\ &= (1 - q_{\Sigma})(1 - q_{\Sigma}) + q_1 R_1 + \dots + q_i R_i + \dots + q_n R_n + 0 \cdot 0, \end{aligned}$$

$$\begin{aligned} P_1(2) &= P_0(1)P_{01} + P_1(1)P_{11} + \dots + P_i(1)P_{i1} + \dots + P_n(1)P_{n1} + P_{n+1}(1)P_{(n+1),1} = \\ &= (1 - q_{\Sigma})q_1 + q_1 \cdot 0 + \dots + q_i \cdot 0 + \dots + q_n \cdot 0 + 0 \cdot 0, \end{aligned}$$

$$P_i(2) = P_0(1)P_{0i} + P_1(1)P_{1i} + \dots + P_i(1)P_{ii} + \dots + P_n(1)P_{ni} + P_{n+1}(1)P_{(n+1),i} = \\ = (1 - q_{\Sigma})q_i + 0 + \dots + 0 + \dots + 0 + 0,$$

$$\dots, \\ P_n(2) = (1 - q_{\Sigma})q_n,$$

$$\dots, \\ P_{n+1}(2) = \sum_{i=1}^n q_i \bar{R}_i.$$

С учетом преобразований вероятности после второго шага будут иметь вид:

$$P_0(2) = (1 - q_{\Sigma})^2 + \sum_{i=1}^n q_i R_i,$$

$$P_1(2) = (1 - q_{\Sigma})q_1,$$

$$P_i(2) = (1 - q_{\Sigma})q_i,$$

$$\dots, \quad (3.7)$$

$$P_n(2) = (1 - q_{\Sigma})q_n,$$

$$\dots, \\ P_{n+1}(2) = \sum_{i=1}^n q_i \bar{R}_i. \quad (3.7)$$

Таким образом, как видно из выражения (3.7), уже после второго шага система может оказаться в поглощающем состоянии, т.е. в состоянии, когда безопасность КИ нарушена.

Используя данный метод, можно провести моделирование процесса функционирования АИС, установить степень взаимосвязи между особенностями деятельности человека-оператора и функциональными особенностями АИС и СЗИ, произвести оценку влияния таких особенностей на итоговый показатель защищенности ИОР.

Результатом проводимого моделирования станет определение вероятности неблагоприятного исхода (нарушение конфиденциальности, целостности, доступности информации) при воздействии на человека-оператора различных дестабилизирующих воздействий в условиях использования технических, программных, аппаратных и иных средств защиты информации в АИС, а также установить степень влияния технических и эргономических свойств СЗИ на вероятность безошибочной работы оператора.