А.П. Росенко, Р.С. Аветисов

Россия, г. Ставрополь, Ставропольский государственный университет

ИССЛЕДОВАНИЕ ВЕЛИЧИНЫ УЩЕРБА ОТ ВОЗДЕЙСТВИЯ НА АВТОМАТИЗИРОВАННУЮ ИНФОРМАЦИОННУЮ СИСТЕМУ ВНУТРЕННИХ УГРОЗ[1]

В связи с постоянно растущим количеством информационных систем в современном обществе и увеличением числа преступлений в этой сфере на первый план выходит проблема оценки величины ущерба от воздействия на информацию различных угроз [1,2]. Для решения данной задачи применяются различные подходы и технологии. Однако, как показывает анализ, наибольшее распространение получают методы математического моделирования.

В статьях [1,2] как раз рассматривается данный вопрос. На основании математической модели определено, что для расчета ущерба необходимо выявить предельные (финальные) вероятности состояний, вычисляемые на каждом уровне иерархической структуры автоматизированной информационной системы (АИС) для каждого из состояний по формуле

$$P_{np} = \prod_{j=1}^{n} \frac{\lambda_{j,j+1}}{\mu_{j+1,j}} \left(1 + \sum_{n=1}^{k-1} \prod_{j=1}^{n} \frac{\lambda_{j,j+1}}{\mu_{j+1,j}} \right)^{-1}, \; n = \overline{1, k-1}, \qquad (1)$$

где параметры $\lambda_{i,i+1}$ и $\mu_{i+1,I}$ определяют число успешных ($\lambda_{i,i+1}$) и неуспешных ($\mu_{i+1,i}$) попыток злоумышленника при переходе системы из состояния i в состояние i+1 и наоборот.

Возникает проблема расчета этих параметров. Для решения данной задачи необходимо получить статистические данные о частоте использования каналов утечки данных, а также определить квалификацию злоумышленника для каждого из каналов утечки.

[1] Работа выполнена при поддержке гранта РФФИ, проект 06-01-00020

Пусть имеется N каналов и известна статистика частоты использования каждого из N каналов – $\delta^k_{i,i+1}$, при переходе из i-го состояния в (i+1)-е, k=1..N. Тогда для определения параметра $\lambda_{i,i+1}$, как показано в [3], целесообразно использовать следующее выражение:

$$\lambda_{i,i+1} = \max_k(t \cdot \delta^k{}_{i,i+1}) \ , \quad k = \overline{1,N}, \tag{2}$$

где t – период моделирования действий злоумышленника.

Пусть имеются данные о квалификации злоумышленника – ω^k, k=1..N. Для удобства расчетов положим, что ω^k принимает значения в интервале [0...1]. Тогда можно записать:

$$\mu_{i+1,i} = \min_k((1-\omega^k) \cdot \lambda_{i,i+1}) \ , \quad k = \overline{1,N} \ . \tag{3}$$

С учетом выражений (1) – (3) можно рассчитать финальную вероятность системы для каждого состояния, а также с учетом методики, предложенной в [1], вероятность реализации несанкционированных действий злоумышленника.

Помимо расчета вероятности реализации несанкционированных действий злоумышленника необходимо определить параметры нормального закона для расчета величины потенциала информации. Как указано в [2], для определения потенциала информации целесообразно использовать формулу

$$U_{общ} = C(\int_t \frac{1}{\sigma_t\sqrt{2\pi}} e^{-(t-a_t)^2/2\sigma_t^2} dt + 1), \tag{4}$$

где C – начальная стоимость информации; t – период жизни (актуальности) информации; параметры σ_t и a_t – параметры нормального закона распределения, описывающие рост и падение потенциальной прибыли от использования информации. Все параметры, используемые в этом выражении, определяются на основе статистики.

Таким образом, если определена потенциальная максимальная стоимость информации, то для определения параметра σ_t можно использовать следующее выражение:

$$\sigma_t = \frac{1}{\sqrt{2\pi} \cdot \frac{C_{\max}}{C}}, \qquad (5)$$

где $C_{\max}$ – прогнозируемая максимальная стоимость информации.

Тогда, используя формулу (5) и определив на основе статистики параметр a_t, можно из (4) определить потенциал информации.

Вышесказанное, а также описание математической модели, предложенное в [2], позволяет построить блок-схему алгоритма нахождения вероятного ущерба.

Блок-схема нахождения ущерба от утечки конфиденциальных сведений в АИС представлена на рис.1. В соответствии с рисунком блок-схема включает 4 функциональных блока.

Первый блок предназначен для расчета стоимости системы защиты $C_{сз}$. Для определения стоимости первоначально вводятся данные о стоимости создания системы защиты $C_{созд}$, а также количество периодов модификации k и обслуживания t. Далее, на основе введенных данных определяются итоговые стоимость обслуживания $C_{обсл}$ и стоимость модификации $C_{мод}$, после расчета которых определяется стоимость системы защиты $C_{сз}$.

На втором функциональном блоке производится расчет потенциала информации $U_{общ}$. Для этого вводится величина, равная потенциальной прибыли от использования информации, а также время ее жизни. Далее на основе выражения (4) производится расчет потенциала информации $U_{общ}$.

Третий блок предназначен для расчета вероятности реализации несанкционированного доступа злоумышленником к конфиденциальной информации $P_{нсд}$. Для этого необходимо определить количество рассматриваемых подсистем иерархической структуры АИС – L и на основе статистических данных о частоте использования каналов утечки рассчитать параметры $\lambda_{i,i+1}$ и $\mu_{i+1,i}$ на основе выражений (2) и (3). Далее на основе полученных данных рассчитывается вероятность реализации несанкционированного доступа .

На четвертом функциональном блоке производится расчет и анализ величины потенциального ущерба U . Среди полученных сведений об ущербе на различных уровнях иерархической структуры АИС выбирается максимум, после чего производится сравнение с величиной допустимого ущерба. Если при этом полученный ущерб больше чем допустимый, то это означает, что система защиты является малоэффективной и требуется ее изменение и проведение новых расчетов, до тех пор, пока величина вероятного ущерба не станет меньше либо равной допустимой.

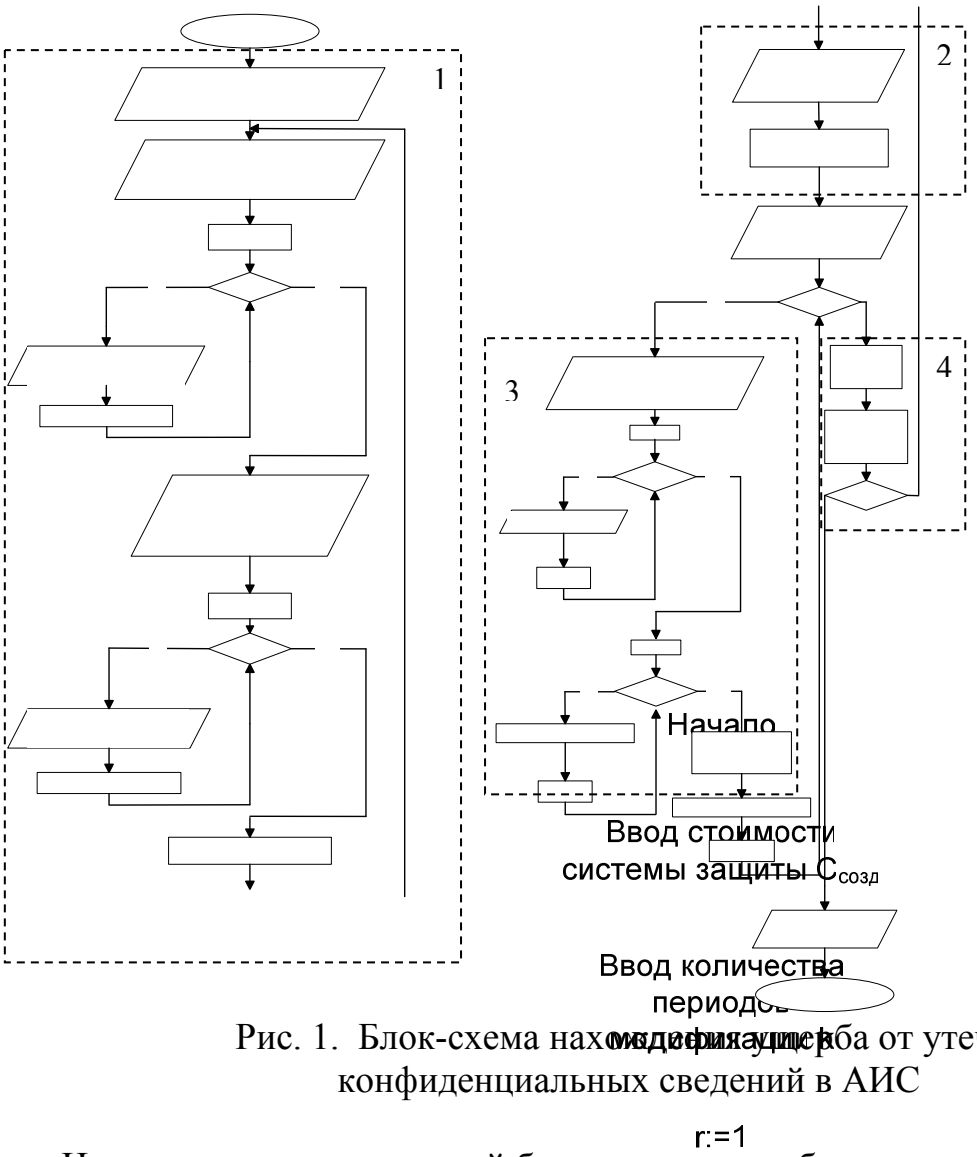

Рис. 1. Блок-схема нахождения ущерба от утечки конфиденциальных сведений в АИС

На основе предоставленной блок-схемы разработана программа по оценке ущерба от утечки конфиденциальных сведений в АИС. При моделировании в качестве начальной стоимости информации была выбрана величина, равная

5000 у.е., что соответствует организации среднего уровня. Результаты моделирования представлены на рис.2 , 3.

На рис.2 представлена зависимость величины ущерба U от квалификации злоумышленника ω. Как видно, эта зависимость носит явно прямопропорциональный характер. Это обусловлено тем, что при одинаковых условиях моделирования величина ущерба, исходя из модели, напрямую зависит от квалификации злоумышленника, так как предполагается равномерное отличие квалификаций злоумышленников различных уровней. Таким образом, можно сделать вывод о том, что зависимость величины ущерба носит тот же характер, что и распределение квалификации злоумышленников.

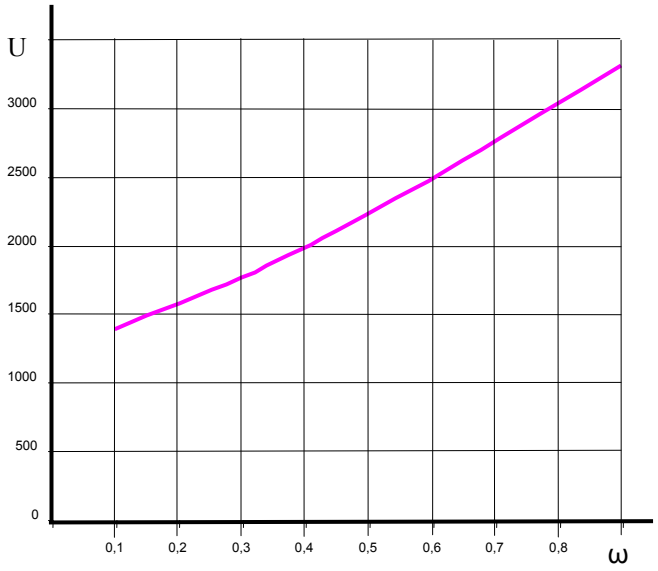

Рис.2. Зависимость величины ущерба U от квалификации злоумышленника ω

На рис.3 представлена зависимости величины потенциального ущерба U от частоты использования канала δ. Данная зависимость имеет экспоненциальный характер. Это объясняется тем, что с ростом частоты использования каналов утечки увеличивается вероятность реализации несанкционированного доступа, так как рост частоты способствует применению большего количества методик несанкционированного доступа злоумышленником.

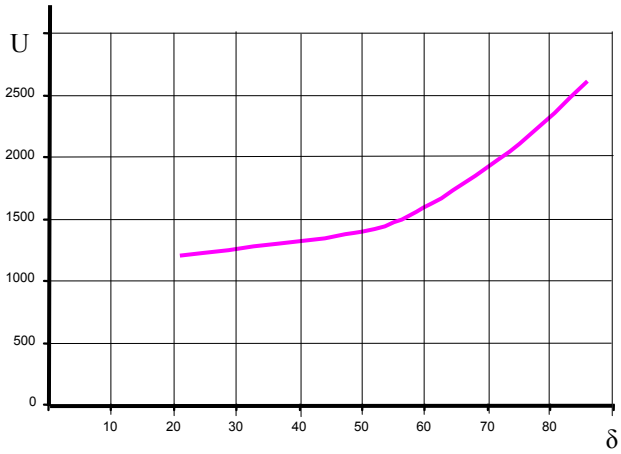

Рис.3 Зависимость величины ущерба U от частоты использования канала δ

Как видно из рис.2, 3, характер зависимости величины ущерба от входных параметров модели является различным. В первую очередь эта зависимость определяется математическими выражениями, описывающими эти параметры, а также их использованием в модели. Поэтому необходимо не только расширять гибкость существующих моделей за счет учета новых параметров, но и улучшать алгоритмы определения поведения этих параметров во времени.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1.*Росенко А.П., Аветисов Р.С.* Методика оценки величины ущерба от воздействия на автоматизированную информационную систему внутренних угроз Известия ТРТУ Тематический выпуск “Информационная безопасность”. – Таганрог, 2006. – С. 33–37.

2.*Росенко А.П., Аветисов Р.С.* Математическая модель исследования величины ущерба от воздействия на конфиденциальную информацию внутренних угроз // Вестник СГУ, Ч 2. – Ставрополь, 2006. – С.23–29.

3.*Росенко А.П., Аветисов Р.С.* Обоснование общей методики оценки влияния внутренних угроз на величину ущерба собственнику конфиденциальной информации. Научно инновационные достижения физико-математического факультета в области физико-математических и технических дисциплин. – Ставрополь: Ставропольское книжное изд-во, 2006. – С. 424–426.