УДК: 004.056

А.Е. Архипов, доктор технических наук, профессор
(Национальный технический университет Украины „КПИ”, Украина)

ВЛИЯНИЕ ЭКОНОМИЧЕСКИХ И ВРЕМЕННЫХ ФАКТОРОВ НА ВЕРОЯТНОСТНЫЕ ПАРАМЕТРЫ МОДЕЛИ УГРОЗ ИНФОРМАЦИИ

Рассматривается методика експертно-аналитического оценивания вероятностных параметров модели „атака-защита”. Методика базируется на анализе экономических мотиваций в системе „атака-защита”.

В работах [1,2] рассматривались некоторые методологические аспекты и формальные приемы, позволяющие получить оценки вероятностных параметров рисков в случае возможной реализации атак (угроз) по отношению к определенному информационному ресурсу защищаемой информационной системы. Отмечалось, что для успешного использования подобных формальных приемов и рекомендаций следует обязательно анализировать реальные особенности рассматриваемых событий (атак, угроз), в частности, экономические мотивации атакующей и защищающейся сторон, а также протяженность (распределенность) этих событий во времени. Ниже исследуются возможности более детального и конкретизированного применение предложенных подходов к решению некоторых практических задач.

Рассмотрим ситуацию, возникающую при реализации атакующей стороной A (злоумышленниками) угрозы T относительно некоторой информации (информационного ресурса) I, принадлежащего стороне B. Полагаем, что D – общая стоимость затрат атакующей стороны A на реализацию угрозы T, g – полученный при этом стороной A «выигрыш», определяемый ценностью информации I для злоумышленников. Урон, причиненный в этой ситуации стороне B, т.е. важность критической информации с точки зрения ее владельца, оценивается им как q, а общая стоимость осуществленного в ИС комплекса защитных мероприятий равняется C.

Приведенные данные дают стоимостную характеристику ситуации «атака-защита». Требуется на базе этих сведений построить логико-эвристическую схему экспертного оценивания вероятностных характеристик, используемых для вычисления информационных рисков.

Очевидно, что активность стороны A в реализации угрозы T определяется в общем случае величиной чистой прибыли

$$Q = g - D, \tag{1}$$

которую сторона A может получить в случае успешной реализации угрозы T. Чем больше прибыль Q, тем устойчивее стремление стороны A к осуществлению угрозы T, которое количественно можно оценить вероятностью угрозы

$$P_N = \frac{g - \alpha D}{g} = 1 - \alpha \frac{D}{g}, \tag{2}$$

где α – некоторый коэффициент, отражающий уровень мотивации стороны A к осуществлению угрозы. Диапазон возможных значений α определяется соотношением

$$1 \le \alpha \le g / D. \tag{3}$$

Однако возможность непосредственной реализации угрозы зависит от уровня защищенности информации I, в частности, от наличия уязвимостей в системе защиты информации (ЗИ) и возможностью проведения стороной A атаки, использующей наличие той или иной уязвимости V. Вероятность успешной реализации этой атаки можно определить выражением:

$$P_V = 1 - \beta \frac{C}{q}, \tag{4}$$

где β – коэффициент, отражающий традиционное для ЗИ соотношение между затратами на защиту стоимостью корпоративной информационной системы (КИС) [3] (либо, по другим источникам, стоимостью защищаемой информации [4], ценностью этой информации [5]): $c = (0{,}05 \div 0{,}25)q$, откуда $\beta = 4 \div 20$. В общем вероятность реализации угрозы (вероятность происшествия, инцидента) определяется как

$$P = P_T P_V . \qquad (5)$$

Следует подчеркнуть, что введение выше вероятности характеризует возможности реализации соответствующих событий в течение некоторого интервала времени τ (конечной или бесконечной длительности), т.е. эти вероятности распределены на интервале времени τ по определенному закону $P(t)$, например [2]:

$$P_T(t) = P_T \int_0^{\tau} p_T(t)dt , \qquad (6)$$

причем $\int_0^{\tau} p_T(t)dt = 1$.

При задании вероятностей $P_T(t)$, $P_V(t)$, названных в [2] терминальными, в качестве распределений $p_T(t)$, $p_V(t)$, могут быть использованы как типовые виды распределений вероятностей, так и специфические, формы которых определяются конкретными особенностями ситуаций, возникающих в ходе развития событий в системе "атака-защита". Рассмотрим несколько вариантов (сценариев) развития подобных событий.

В первом варианте будем полагать, что атакующая сторона A имеет устойчиво постоянный интерес к информации I, владельцем которой является защищающаяся сторона В, причем время существования этого интереса $t_{\max}$ зависит только от величины суммарных затрат $D(t)$, понесенных атакующей стороной A на подготовку, организацию и проведение атакующих действий. Если в некоторый момент времени $t_{\max}$ величина суммарных затрат $D(t_{\max})$ достигнет значения, при котором $\alpha D(t_{\max})/g$ станет равным 1, то в соответствии с формулой (2) терминальная вероятность $P_T(t_{\max})$ окажется равной 0, т.е. дальнейшее продолжение атакующих действий стороной A представляется нерациональным. Затраты $D(t_{\max}) = D_{\max}$ назовем предельно возможными затратами стороны A. Предположим далее, что текущие затраты δ атакующей стороны в среднем неизменны во времени. Тогда справедливы соотношения:

$$D(t) = \delta t \le D_{\max} , \qquad t_{\max} = D_{\max} / \delta , \qquad (7)$$

где $t_{\max}$ – длительность интервала времени, в течение которого сторона А полностью расходует свой атакующий ресурс и прекращает попытки реализации угрозы Т по отношению к информации I, владельцем которой является сторона B.

Значение терминальной вероятности $P_T(t)$ в соответствие с выражениями (2), (7) определяется формулой:

$$P_T(t) = (1 - \alpha \frac{\delta}{g} t) . \qquad (8)$$

Кроме того будем полагать, что с ростом общего времени t, которое сторона A тратит на организацию, подготовку и проведение атак (т.е. по мере накопления стороной A опыта реализации угрозы и сведений о системе ЗИ стороны B), растет терминальная вероятность $P_V(t)$ успешного использования стороной A уязвимости V: $P_V(t)=p_v(t)$, где p_v=const. Тогда вероятность происшествия (реализация угрозы) определяется выражением:

$$P(t) = P_T(t)P_V(t) = (1 - \alpha \frac{\delta}{g} t) p_V t = p_V t - \frac{\alpha \delta p_V}{g} t^2 . \qquad (9)$$

При этом вероятность $P(t)$ возрастает, начиная от $P(0)=0$ до своего максимального значения $P(t_{extr}) = 0{,}25 p_V g / \alpha\delta$, соответствующего моменту времени $t_{extr} = g / 2\alpha\delta$, уменьшаясь затем вновь до *0*: $P(t_{\max})=0$.

Для второго сценария развития событий в системе "атака-защита" доминирующим является влияние фактора времени на мотивацию и действия атакующей стороны *A*. В частности предполагается, что доступ к информации *I* возможен только в течение ограниченного интервала времени (*0*, t_0], т.е. $P(t)=0$ при $t>t_0$. В этой ситуации мотивация атакующей стороны *A* резко возрастает по мере приближения момента t_0 (если ранее предпринимаемые атаки окончились неудачей), что отображается моделью вида:

$$P_T(t) = \frac{P_{T\max}}{t_0 - t + 1}, \qquad P_{T\max} = P_T(t_0). \tag{10}$$

Очевидно, что рост мотивации должен обуславливать рост ресурсов, привлекаемых стороной *A* для подготовки, организации и реализации атак, при этом зависимость $D(t)$ будет отличаться от линейной, представленной в соотношении (7). Если значение $D_{\max}$ задано, из уравнения (2) можно найти

$$P_{T\max} = 1 - \alpha \frac{D_{\max}}{g}, \tag{11}$$

и, приравняв выражения (2), (10), определить, с учетом равенства (11), зависимость $D(t)$:

$$\frac{P_{T\max}}{t_0 - t + 1} = 1 - \alpha \frac{D(t)}{g}, \tag{12}$$

$$D(t) = \frac{g}{\alpha}\left(1 - \frac{P_{T\max}}{t_0 - t + 1}\right) = \gamma\left(1 - \frac{1 - \gamma D_{\max}}{t_0 - t + 1}\right),$$

где $\gamma = g / \alpha$. Начальные затраты стороны *A* на атакующие действия составят:

$$D(0) = \frac{\gamma t_0}{t_0 + 1}\left(1 + \frac{D_{\max}}{\gamma t_0}\right). \tag{13}$$

Выводы

Анализ экономико-стоимостных соотношений в системе «атака-защита» при исследовании угроз информации позволяет построить эвристические модели для оценивания вероятностей угроз информации и уязвимости информационных ресурсов. Получаемые при этом оценки вероятностей могут быть как сосредоточенными (точечными), так и распределенными на некотором временном интервале, а также менять свои значения в зависимости от характера развития событий в системе "атака-защита".

Список литературы

1. *Архипов А.Е., Архипова С.А.* Применение мотивационно-стоимостных моделей для описания вероятностных соотношений в системе «атака-защита». - Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Київ-2008р, випуск 1(16).- с. 57-61.

2. *Архипов А.Е.* Об особенностях оценивания вероятностей, используемых для вычисления информационных рисков. - Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту: Матеріали міжнародної наукової конференції (ISDMCI '2010). Том 2. – Херсон: ХНТУ, 2010. – 590с, с.515-517..

3. *Петренко С.А., Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. М.: Компания Ай Ти; ДМК Пресс, 2004. - 348с.

4. *Андрощук Г.А., Крайнев П.П.* Экономическая безопасность предприятия: защита коммерческой тайны. – К.: Изд. Дом «Ин Юре», 2000. – 400с.11. Толстова Ю.Н. Измерение в социологии.- М.: ИНФРА – М, 1998. – 224с.

5. *Гринберг А.С., Горбачев Н.Н., Тепляков А.А.* Защита информационных ресурсов государственного управления. – М.: Юнити-ДАНА, 2003. – 327с.