УДК 004.056

Архипов А.Е. (НТУУ «КПИ»)

ПРИМЕНЕНИЕ ЭКОНОМИКО-МОТИВАЦИОННЫХ СООТНОШЕНИЙ ДЛЯ ОЦЕНИВАНИЯ ВЕРОЯТНОСТНЫХ ПАРАМЕТРОВ ИНФОРМАЦИОННЫХ РИСКОВ

В статье проведен анализ экономико-стоимостных соотношений в системе «атака-защита» при исследовании угроз информации, что даст возможность построить эвристические модели для оценивания вероятностей угроз информации и уязвимости информационных ресурсов.

Ключевые слова: информационный риск, угроза, уязвимость, эвристическая модель, «атака-защита».

На сегодняшний день наиболее эффективным подходом к проектированию и исследованию систем защиты информации (СЗИ) в информационных системах (ИС) считается метод анализа информационных рисков [1-4]. В основе методологии информационных рисков лежит измерение рисков угроз защищенности информации, обрабатываемой в ИС. Существуют различные способы измерения информационных рисков. На практике чаще всего применяют так называемые табличные методы нахождения рисков, использующие качественные шкалы для оценивания вероятностных характеристик угроз и степени тяжести последствий, наступающих в случае реализации этих угроз [1,2]. Табличные методы удобны и достаточно адекватны задачам, решаемым на ранних стадиях проектирования СЗИ, в частности, на этапе предпроектных исследований.

Однако по мере конкретизации структуры СЗИ, детализации механизмов защиты, средств и элементов, реализующих эти механизмы, появляется необходимость в более точном измерении рисков, требующем применение количественных шкал для оценивания вероятностных параметров угроз и уязвимостей ИС, определения ущерба, в частности, стоимости потерь, обусловленных успешной реализацией угроз. Особенно актуальным данное требование становится при оценивании остаточных рисков, характеризующих степень эффективности СЗИ, при решении задачи оптимизации выбора механизмов и средств защиты информации в ИС. В этой ситуации для получения количественных оценок обычно используются экспертные методы (индивидуальные или групповые эксперты) [2]. Наибольшее распространение получили групповые методы экспертного оценивания, в которых эксперт непосредственно указывает количественные значения анализируемых параметров: вероятностей, ущерба, стоимости потерь и т.п. Менее известны экспертно-аналитические методы получения оценок, базирующиеся на применении логико-эвристических схем (конструкций, моделей), с помощью которых эксперт пытается упорядочить, по возможности логически увязать совокупность разрозненных, часто неполных сведений в сфере проводимой экспертизы и в конечном итоге получить искомые оценочные суждения относительно анализируемых параметров (характеристик).

В частности, при оценивании вероятностных характеристик угроз, используемых для вычисления информационных рисков, можно применить стоимостные схемы, имеющие место в ситуации «атака-защита» ИС. Так, в [5, стр. 263] отмечается, «что как затраты на атаку, так и затраты на защиту от возможных атак следует соотносить со стоимостью защищаемых ресурсов». В [6, стр. 66] для получения характеристик интенсивности потока угроз авторы предлагают применить так называемый оптимистически-пессимистический подход, основывающийся на существовании прямой пропорциональности между интенсивностью потока угроз и обусловленных их реализацией потерь (ущерба): «чем больше потери от взлома (успешной атаки), тем чаще осуществляются попытки несанкционированного доступа (НСД) к этой информации». В [7] предпринята попытка игровой интерпретации финансово-экономических интересов злоумышленника и владельца критической информации в ситуации «атака-защита». Следует отметить, что не все из приведенных выше схем удачны или хотя бы допускают рациональную интерпретацию.

Например, при проведении атак на ресурсы ИС атакующую сторону к повторению попыток НСД будут стимулировать размеры выгоды, полученной в случае успешного завершения атаки, тогда как возникшие при этом потери касаются исключительно владельца ИС и, скорее всего, подтолкнут его к усилению уровня защищенности ИС.

В целом наличие подобных логико-эвристических схем позволяет надеяться на более обоснованные и более высокоточные экспертные оценки, получаемые экспертно-аналитическим методом, по сравнению с другими способами осуществления экспертизы.

Рассмотрим ситуацию, возникающую при реализации атакующей стороной A (злоумышленники) угрозы T относительно некоторого информационного ресурса I, принадлежащего стороне B. Полагаем, что D – общая стоимость затрат атакующей стороны A на реализацию угрозы T, g – полученный при этом «выигрыш», определяемый ценностью ресурса I для злоумышленников. Урон, причиненный в этой ситуации стороне B (владельцу ресурса I), т.е. стоимость 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 чистая прибыль злоумышленников в случае успешной реализации угрозы T составит:

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

Если интерес атакующей стороны A к критической информации I носит не разовый, а долговременный характер, т.е. можно предположить, что $g=const$, естественной является мотивация злоумышленников к уменьшению значений D (росту прибыли Q). При этом интенсивность потока попыток доступа злоумышленников к ресурсу I будет возрастать, а вероятность угрозы T можно будет оценить выражением:

$$P_T = (1 + \frac{D}{Q})^{-1} = 1 - \frac{D}{g}. \tag{2}$$

Возможен еще один, более гибкий вариант задания вероятности P_T с введением коэффициента γ, отражающего уровень мотивации стороны A к осуществлению угрозы:

$$P_T = \frac{g - D/\gamma}{g} = 1 - \frac{D}{\gamma g} \tag{3}$$

Диапазон возможных значений γ определяется соотношением $D/g \le \gamma \le 1$.

Ясно, что если ценность ресурса I для атакующей стороны A очень высока, злоумышленники готовы идти на значительные затраты средств для реализации угрозы T. Поэтому в случае $g>>D$ вероятность P_T будет практически равна 1. При малых значениях g мотивированность злоумышленников к реализации угрозы T низка, в частности при Q=0 (т.е. $g=D$) теоретически $P_T = 0$, а при $g<D$ формула (2) теряет смысл. На практике это означает, что вероятность применения для реализации угроз высокозатратных атак низка. Атаки, подготовка, организация и проведение которых сопряжена со значительными затратами, оправданы лишь в случае, если, например, информация I составляет государственную тайну, т.е. уровень ее критичности может быть чрезвычайно высок и даже для больших значений D выполняется неравенство $D/g<1$. Кроме того, важным аспектом в анализе вероятности затратных атак является то, что их организация и проведение связаны со значительными финансовыми рисками, позволить которые себе могут далеко не многие фирмы или организации.

Мотивацию действий владельца информации (сторона *B*) по защите *I* можно проанализировать, введя понятие вероятности безопасности критической информации по отношению к угрозе *T*:

$$P_S = (1 + \frac{q}{sc})^{-1} = \frac{sc}{q + sc}, \quad (4)$$

где *s* – некоторый коэффициент, необходимость введения которого рассмотрим ниже. Как следует из формулы (4), вероятность P_S =1 при *q*=0, т.е. критическая информация в ИС отсутствует. При *q*>>*sc*, т.е. при значительном уровне критичности ресурса *I* и низких затратах на создание и функционирование СЗИ, следствием чего является объективная невозможность обеспечить адекватный уровень защиты критической информации в ИС, вероятность $P_S \to 0$.

Для достижения требуемого уровня защищенности необходимо нейтрализовать имеющиеся в ИС уязвимости, повысив эффективность функционирования СЗИ. Это неминуемо повлечет увеличение затрат *c* на реализацию дополнительных защитных мероприятий и *sc* станет сопоставимым с *q*. Естественно, что рост затрат *c* должен происходить в условиях рационального расходования выделенных на совершенствование СЗИ средств и правильно скорректированной политике безопасности ИС.

Рассмотрим причины введения коэффициента *s* в формуле (4) и определимся с его значением. Обычно ресурс *I* является одним из множества информационных элементов, составляющих общий информационный ресурс *I*. Учитывая, что СЗИ защищает не каждый ресурс в отдельности, а всю их совокупность в целом, стоимость защитных мероприятий оказывается ниже значения *q*. Из практики разработки и построения СЗИ известно, что стоимость затрат на защиту в большинстве случаев не должна превышать 10% цены защищаемого ресурса [5] (по другим данным – 5÷15% [1]). Наиболее конкретные сведения приведены в [8], согласно которым P_S ≈0,5 при *c=0,1q* и P_S ≈0,9 при *c=(0,15÷0,2)q*. Перечисленные условия удовлетворяются при различных значениях s, лежащих в диапазоне 10÷50. Далее в качестве константы *s* в формуле (4) предлагается использовать *s*=30.

Вероятность безопасности ресурса *I* по отношению к угрозе *T* связана с вероятностью P_V наличия уязвимостей ИС, способствующих реализации угрозы *t*, очевидным соотношением $P_S + P_V = 1$, откуда

$$P_V = 1 - P_S = \frac{q}{q + sc}. \quad (5)$$

Приведенные выше формулы (2), (4) позволяют оценить, исходя исключительно из стоимостных характеристик ситуации «атака-защита», значения вероятностей угрозы P_t и уязвимости P_V, необходимые для вычисления информационного риска по так называемой трехфакторной формуле [1]:

$$R_t = P_V P_t q = \frac{q^2 (g - D)}{g (q - sc)}, \quad (6)$$

где произведение $P_V P_T$ определяет вероятность успешной реализации угрозы *T*.

Рассмотрим некоторые дополнительные возможности, возникающие при оценивании параметров риска, в частности, вероятности P_V, исходя из условия рационального расходования средств на построение СЗИ.

При полном отсутствии СЗИ очевидно, что $P_v = 1$, и информационный риск $R_I = P_T q$. Если стороной *B* инвестированы в СЗИ определенные средства в размере c единиц, то при условии их рационального расходования вероятность реализации уязвимости станет меньше 1, т.е. P_v <1. Величина потерь, которые удалось предупредить введением СЗИ, составляет:

$$R_1 - R = P_t q - P_t P_v q = (1 - P_v) P_t q = P_s P_t q \ . \quad (7)$$

Если затраты на защиту – c, то «доход» от введения защиты равен

$$\Delta_R = R_1 - R - c = (1 - P_v) P_t q - c = P_s P_t q - c \ . \quad (8)$$

Заменяя P_s его развернутым выражением (3), получаем:

$$-c + \frac{sc}{q + sc} P_t q = \Delta_R \ , \quad (9)$$

Из анализа выражения (9) следует, что если уровень инвестиций c превышает некоторое предельное значение $c_{max} = q(P_T s - 1)/s$, "доход" от введения защиты становится отрицательным, т.е. в общем случае диапазон возможных значений c рационально ограничить условием:

$$0 < c < q(P s - 1)/s. \quad (10)$$

Оценим уровень инвестиций в СЗИ, при котором значение Δ_R оказывается наибольшим:

$$\frac{d\Delta_R}{dc} = \frac{s(q + sc) - s^2 c}{(q + sc)^2} P_t q - 1 = 0 \ ,$$

$$\frac{sq}{(q + sc)^2} P_t q = 1 \ ,$$

$$P_t s q^2 = q^2 + 2sqc + s^2 c^2 \ ,$$

$$c^2 + 2\frac{q}{s} c + \frac{q^2}{s^2}(1 - P_t s) = 0 \ ,$$

$$c = -\frac{q}{s} \pm \sqrt{\frac{q^2}{s^2} - \frac{q^2}{s^2}(1 - P_t s)} = -\frac{q}{s} \pm \sqrt{P_t s}\,\frac{q}{s} = -\frac{q}{s}(1 \pm \sqrt{P_t s}) \ . \quad (11)$$

По своему содержанию затраты c не могут быть отрицательными, поэтому в соотношении (11) выражение в круглых скобках должно быть меньше нуля. С учетом этих требований

$$c = \frac{q}{s}(\sqrt{P_t s} - 1) \ . \quad (12)$$

Подставим найденное выражение (12) в уравнение (5) для вероятности P_v :

$$P_v = \frac{q}{q - q(1 - \sqrt{P_t s})} = \frac{1}{1 - 1 + \sqrt{P_t s}} = \frac{1}{\sqrt{Ps}} \ . \quad (13)$$

Учитывая что $P_v \le 1$, получаем: $1 \ge \frac{1}{\sqrt{P_T s}}$, откуда $\sqrt{P_T s} \ge 1$, значит $s \ge \frac{1}{P_T}$ или окончательно: $1 > P_T > \frac{1}{s}$, а подстановка (13) в выражение (6) позволяет получить значение риска при объеме инвестиций $c = c_{extr}$:

$$R_T(c_{extr}) = P_V P_T q = q\sqrt{\frac{P_T}{s}} \ . \quad (14)$$

Для крайней правой точки c_{max} интервала (10) получаем: $P_V(c_{\max}) = \frac{1}{P_T s}$,

$P_T(c_{\max}) = \frac{q}{s}$.

Особенностью полученных выше результатов является то, что все они опираются на гипотезу статичности, постоянства во времени экономико-мотивационных показателей системы "атака-защита". Однако в реальности для этой системы свойственно динамичное развитие ситуации, сопровождающееся постоянным изменением ее стоимостных и мотивационных характеристик, что обуславливает изменчивость как вероятностных параметров информационного риска, так и его собственных значений. Фактически информационный риск является динамичным (процессным) показателем, требующим для своего анализа и описания подходов, выходящих за рамки традиционной статичной схемы.

Попытка решения этой проблемы была предпринята в [10], где предлагается ввести так называемую терминальную вероятность $P(t)$, распределенную на интервале времени τ конечной или бесконечной длительности, текущие значения которой используются как значения вероятности при вычислении информационного риска $R(t)$ в соответствующей точке t этого интервала. Применим терминальную вероятность для описания экономико-мотивационных соотношений в системе «атака-защита».

Как отмечалось выше, величина вероятности P реализации угрозы T со стороны A относительно информации I, находящейся во владении стороны В, зависит от действия двух факторов:

– наличия у стороны A интереса к информации I, собственно и инициирующее возникновение угрозы T;

– уровня защищенности информации I в системе "атака-защита", в частности, наличие в СЗИ уязвимостей, допускающих возможность реализации угрозы T.

Выраженность и интенсивность действия этих факторов в пределах возможных значений τ определяется распределением на интервале τ соответствующих терминальных вероятностей $P_T(t)$, $P_V(t)$. Учитывая независимость действия рассмотренных факторов, представим вероятность $P(t)$ в виде произведения: $P(t)=P_T(t)P_V(t)$.

Терминальные вероятности $P_T(t)$, $P_V(t)$ могут задаваться как соответствующими функциями распределения $p_t(t)$, $p_v(t)$, так и путем непосредственного задания значений функций $P_T(t)$, $P_V(t)$, вид которых определяется конкретными особенностями ситуаций, возникающих в ходе развития событий в системе "атака-защита". Рассмотрим несколько вариантов (сценариев) развития подобных событий [11].

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 при подготовке, организации и проведении атакующих действий. Если в некоторый момент времени $t_{\max}$ величина суммарных затрат $D(t_{\max})$ достигнет значения, при котором $D(t_{\max})/\gamma g$ станет равным 1, то в соответствии с формулой (3) 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:

$$D(t) = \delta t \le D_{\max}, \qquad t_{\max} = D_{\max}/\delta, \tag{15}$$

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

Значение терминальной вероятности $P_T(t)$ в соответствие с выражениями (3), (15) определяется формулой:

$$P_T(t) = (1 - \frac{\delta}{\gamma g} t). \quad (16)$$

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. Таким образом, считаем, что плотность вероятности $p_v(t)$ распределена равномерно в промежутке $(0, t_v)$, $t_v > t_{max}$. Тогда вероятность происшествия (реализация угрозы) определяется выражением:

$$P(t) = P_T(t) P_V(t) = (1 - \frac{\delta}{\gamma g} t) p_v t = p_v t - \frac{\delta p_v}{\gamma g} t^2. \quad (17)$$

При этом вероятность $P(t)$ возрастает, начиная от $P(0)=0$ до своего максимального значения $P(t_{extr}) = 0{,}25 p_V \gamma g / \delta$, соответствующего моменту времени $t_{extr} = \gamma g / 2\delta$, 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 $(0, t_{max}]$, т.е. $P(t)=0$ при $t > t_{max}$. Кроме того, предполагается, что в этой ситуации мотивация атакующей стороны A резко возрастает по мере приближения момента t_{max} (если ранее предпринимаемые атаки окончились неудачей), что отображается моделью вида:

$$P_T(t) = \frac{P_{T\max}}{t_{\max} - t + 1}, \qquad P_{T\max} = P_T(t_{\max}). \quad (18)$$

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 соотношениях (15).

Механическое объединение формул (16) и (18) приводит к выражению

$$P_T(t) = \frac{P_{T\max}}{t_{\max} - t + 1} = 1 - \frac{D(t)}{\gamma g}, \quad (19)$$

абсурдному по своей сути: согласно правой части равенства (19) рост вероятности $P_T(t)$ по мере приближения к моменту t_{max} может быть обусловлен только уменьшением ресурса $D(t)$, который на практике должен с течением времени возрастать адекватно росту мотивации атакующей стороны A. Очевидно, что в этом случае для получения рационального объяснения равенства (19) при описании $P_T(t)$ следует учесть текущее изменение (рост) мотивационных установок атакующей стороны введением изменяющегося во времени коэффициента мотивации $\gamma(t)$. Тогда

$$P_T(t) = 1 - \frac{D(t)}{g\gamma(t)}. \quad (20)$$

При этом изменение коэффициента мотивации во времени определяется выражением

$$\gamma(t) = \frac{1}{g} \frac{D(t)}{1 - P_T(t)}, \quad (21)$$

для которого правая граница γ_{max} возможных значений коэффициента $\gamma(t)$ смещается в бесконечность.

В частности, при равномерном выделении ресурсов атакующей стороной, т.е. для $D(t) = t\delta$, получаем:

$$\gamma(t) = \frac{\delta t}{g} \cdot \frac{1}{1 - P_T(t)} = \frac{\delta t}{g} \cdot \frac{t_{\max} - t + 1}{t_{\max} - t + 1 - P_{T\max}}, \qquad (22)$$

где для $0 < P_{max} < 1$ получаем: $\gamma_{max} = \gamma(t_{max})$ и $\delta t_{max} / g < \gamma_{max} < \infty$.

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".

Литература

1. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: Компания Ай Ти; ДМК Пресс, 2004. - 348с.
2. Симонов С.В. Методология анализа рисков в информационных системах// Конфидент. Защита информации. - №2. – 2001. – с. 48-53.
3. Петренко С.А., Петренко А.А Аудит безопасности Intranet. –М.: ДМК Пресс, 2002. –416с.
4. Архипов А.Е. Применение среднего риска для оценивания эффективности защиты информационных систем.// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.// науково-техн. зб. – Київ, 2007. – Вип.1(14). – с.60-67.
5. Гринберг А.С., Горбачев Н.Н., Тепляков А.А. Защита информационных ресурсов государственного управления. – М.: Юнити-ДАНА, 2003. – 327с.
6. Щеглов Ю.А. Защита компьютерной информации от несанкционированного доступа.- СПб: Наука и техника, 2004-384с.
7. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Кн..1. – М.: Энергоатомиздат, 1994. – 400с.
8. Андрощук Г.А., Крайнев П.П. Экономическая безопасность предприятия: защита коммерческой тайны. – К.: Изд. Дом «Ин Юре», 2000. – 400с.
9. 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.
10. 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.
11. Архипов А.Е. Построение сценариев реализации угроз информации с использованием экономико-мотивационных соотношений. - Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту: Матеріали міжнародної наукової конференції (ISDMCI '2011). Том 1. – Херсон: ХНТУ, 2011. – 472с, с.344-346.

Надійшла: 02.06.2011 р.

Рецензент: д.т.н., проф. Корченко О.Г.