– про потенційно можливі загрози інформації, а також можливі наслідки їх реалізації.

Основу другої групи складають моніторингові дані, пріоритетні завдання, рекомендації.

Подальшим напрямком досліджень є визначення структури та змісту основних задач управління, які зазначені в структурі системи підтримки прийняття рішення.

Висновки

Таким чином, визначена структура системи підтримки прийняття рішення процесу управління захистом інформації в ІТС, що базується на адаптивній моделі системи інформаційної безпеки. Це дозволяє реалізацію наступної послідовності заходів: оцінку фактичного стану інформаційної безпеки ІТС, прогнозування стану інформаційної безпеки системи й ступеню впливу загроз і дестабілізуючих чинників, планування системи заходів захисту інформації відповідно до факторів загроз і поточних значень захищеності системи, визначення методів і механізмів забезпечення необхідного рівня захищеності та прийняття рішення щодо управління системою захисту інформації.

Література: ***1.*** *Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. – С.Пб., 2004. – 384 с.* ***2.*** *Щеглов А. Ю. Проблемы и принципы проектирования систем защиты информации от НСД. // "Экономика и производство",№ 3 – М.: 2001. – С. 34 – 46.* ***3.*** *Вертузаев М. С., Юрченко О. М. Защита информации в компьютерных системах от несанкционированного доступа. – К., 2001. – 321 с.* ***4.*** *Осовецкий Л., Шевченко В. Оценка защищенности сетей и систем // Экспресс электроника, № 2-3, 2002. – С.20-24.* ***5.*** *Жижелев А. В., Панфилов А. П., Язов Ю. К., Батищев Р. В. К оценке эффективности защиты информации в телекоммуникационных системах посредством нечетких множеств //. Приборостроение. 2003. – Т. 46, № 7. – С. 22-29.* ***6.*** *Карпычев В. Ю., Минаев В. А. Цена информационной безопасности // Системы безопасности. № 5, 2003. – С. 128-130.* ***7.*** *Девянин П. Н. и др. Теоретические основы компьютерной безопасности. – М.: ,,Радио и Связь", 2000. – 352 с.* ***8.*** *Партыка Т. Л., Попов И. И. Информационная безопасность. Учебное пособие. М.: ФОРУМ: ИНФРА-М, 2002. – 368 с.* ***9.*** *Габарчук В., Зинович З., Свиц А. Кибернетический подход к проектированию систем защиты информации. – К.: Киев-Луцк-Любляны, 2003. – 653 с.* ***10.****. Нестерук Г. Ф., Осовецкий Л. Г., Нестерук Ф. Г. Адаптивная модель нейросетевых систем информационной безопасности // Перспективные информационные технологии и интеллектуальные систем, № 3 (15), 2003.– С. 14-16.* ***11.*** *Нестерук Г. Ф., Осовецкий Л. Г., Нестерук Ф. Г. К оценке защищенности систем информационных технологий // Перспективные информационные технологии и интеллектуальные системы. № 1, 2004. – С. 48-54.* ***12.*** *Петров В. А., Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.: ил.* ***13.*** *Бриль В. М. К построению рациональной системы управления защитой информации в системах обработки данных. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. К.: – 2003. – С. 199-201.* ***14.*** *Бриль В. М., Нестеренко С. Д., Шаталюк В. В. Оценка показателей уязвимости информации при несанкционированном доступе. Научный сборник "Защита информации", К.: – 2000. – 156 с.* ***15.*** *Герасимов Б. М., Дивизюк М. М., Субач И. Ю. Системы поддержки принятия решений: проектирование, применение, оценка эффективности. Севастополь. – 2004. – 318 с.*

УДК 004.056

ПРИМЕНЕНИЕ МОТИВАЦИОННО-СТОИМОСТНЫХ МОДЕЛЕЙ ДЛЯ ОПИСАНИЯ ВЕРОЯТНОСТНЫХ СООТНОШЕНИЙ В СИСТЕМЕ «АТАКА-ЗАЩИТА»

Александр Архипов, София Архипова

Национальный технический университет Украины ,,КПИ"

Анотація: **Розглядається методика експертно-аналітичного оцінювання параметрів системи „атака-захист". Методика базується на аналізі витратно-вартісних мотивацій суб'єктів.**

Summary: **The technique of expert-analytical evaluation of parameters of system "attack – protection" is examined. The technique is based on the analysis of expenditure / cost motivations of subjects of this system.**

Ключові слова: **Вартість втрат, витрати на захист, витрати на атаку, ймовірність загрози, ймовірність атаки, експертне-аналітичне оцінювання, витратно-вартісні мотивації**.

I Введение

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, 5, 6]. 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 составляемых экспертом логико-эвристических схем (конструкций, моделей), с помощью которых он пытается упорядочить и по возможности логически увязать совокупность разрозненных и часто неполных сведений в сфере проводимой экспертизы. Параметры этих схем или их соотношения задаются экспертным путем, позволяя в конечном итоге получить искомые оценочные суждения относительно анализируемых 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 [7, стр. 263] отмечается, «что как затраты на атаку, так и затраты на защиту от возможных атак следует соотносить со стоимостью защищаемых ресурсов». В [8, 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 [9] 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.

II Постановка задачи

Рассмотрим ситуацию, возникающую при реализации атакующей стороной (злоумышленниками) угрозы t относительно некоторого информационного ресурса I. Полагаем, что D – общая стоимость затрат атакующей стороны на реализацию угрозы t, g – полученный при этом «выигрыш», определяемый ценностью ресурса I для злоумышленников. Урон, причиненный в этой ситуации владельцу ресурса I, т. е. стоимость критической информации с точки зрения ее владельца оценивается им как g, 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.

III Мотивационно-стоимостные модели действий атакующей и защищающейся сторон

Очевидно, что чистая прибыль злоумышленников в случае успешной реализации угрозы *t* составит:

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

а эффективность их действий можно оценить отношением

$$E_t = \frac{Q}{D} = \frac{g}{D} - 1. \tag{2}$$

Если интерес атакующей стороны к критической информации *I* носит не разовый, а долговременный характер, т. е. можно предположить, что *g=const*, то 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:

$$P_t = (1 + E_t^{-1})^{-1} = (1 + \frac{D}{Q})^{-1} = 1 - \frac{D}{g}. \tag{3}$$

Ясно, что если ценность ресурса *I* для атакующей стороны 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 (3) 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 значительных *D* (*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 (владельца ИС) по защите *I* можно проанализировать, введя понятие вероятности безопасности критической информации по отношению к угрозе *t*:

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

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 [7] (по другим данным – 5÷15% [1]). Наиболее конкретные сведения приведены в [24], 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) будем 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

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

Если по аналогии с формулой (2) ввести понятие эффективности защиты $E_v = q / C$, выражение (5) можно представить в виде:

$$P_V = 1 - \frac{S}{E_V + S} = \frac{E_V}{E_V + S}. \quad (6)$$

При проведении практических расчетов оценивание вероятностей P_t, P_V через значения эффективностей E_t, E_V имеет определенные преимущества по сравнению с соотношениями, содержащими в своем составе стоимостные показатели *g, q, D, C*. Во-первых, исчезает необходимость в нахождении прямых количественных значений этих показателей и, в частности, в выборе единиц измерения. Во-вторых, эффективности E_t, E_V – оценки относительной ценности, для получения которых можно применить метод парных сравнений, дающий достаточно надежные результаты [11].

Приведенные выше формулы (3), (5) позволяют оценить, исходя исключительно из стоимостных характеристик ситуации «атака-защита», значения вероятностей угрозы P_t и уязвимостей P_V, необходимые для вычисления информационного риска по так называемой трехфакторной формуле [1]:

$$R_t = P_V P_t q = \frac{q^2 (g - D)}{g(q - SC)}, \quad (7)$$

где произведение $P_V P_t$ определяет вероятность успешной реализации угрозы *t*.

Структура выражений (3), (6) являющихся эвристическими моделями, определяется мотивационными аспектами действий атакующей и защищающейся сторон, обусловленными экономико-стоимостными факторами.

При детализации действий атакующей и защищающейся сторон до уровня отдельных уязвимостей и атак и возможности получения на этом уровне соответствующих экономико-стоимостных описаний изложенный выше подход к оцениванию вероятностей P_t и P_V можно распространить на получение оценок вероятностей атак и вероятностей уязвимостей. Так, располагая сведениями о совокупности возможных атак $A = \{a_1, ..., a_i, ..., a_N\}$, позволяющих реализовать угрозу *t*, и стоимостей $d = \{d_1, ..., d_N\}$ на организацию и проведение каждой из них, можно, по аналогии с (3), рассчитать вероятности $p(a_i)$, $i = \overline{1, N}$ этих атак:

$$p(a_i) = 1 - \frac{d_i}{g} = \frac{1}{1 + E_{t_i}^{-1}}. \quad (8)$$

При наличии списка возможных уязвимостей ИС $V = \{v_1, ..., v_j, ..., v_H\}$ и справедливости предположения о том, что стоимость затрат на защитные мероприятия *C* допускает фрагментирование на неравные доли $c_1, c_2, ..., c_H$ соответственно элементам этого списка, вероятности уязвимостей можно определить по формуле, аналогичной (6):

$$p(v_j) = \frac{q}{q + Sc_j}, \quad j = \overline{1, H}. \quad (9)$$

При определении вероятностей $p(a_i)$ и $p(v_j)$ в максимальной степени проявляются преимущества использования оценок эффективности E_{t_i}, E_{v_j}, вычисляемых методом парных сравнений, который обеспечивает возможность применения общей базы сравнения для соответствующих классов оценок («выигрыша» *g* для множества оценок $E_{t_i} = d_i / g$ и потерь *q* для множества оценок $E_{v_j} = C_j / q$).

Обобщая информацию, содержащуюся в совокупностях рассчитанных значений $\{p(a_i)\}$, $i = \overline{1, N}$ и $\{p(v_j)\}$, $j = \overline{1, H}$, получим оценки вероятности угрозы *t*

$$P_t^* = 1 - \prod_{i=1}^{N} (1 - p(a_i)) \tag{10}$$

и вероятности уязвимости ИС относительно этой угрозы:

$$P_V^* = 1 - \prod_{j=1}^{H} (1 - p(v_j)) = 1 - \prod_{j=1}^{H} p_S(v_j), \tag{11}$$

где

$$p_S(v_j) = 1 - p(v_j) = \frac{Sc_j}{q + Sc_j} \tag{12}$$

– безопасность ресурса *I* по отношению к уязвимости v_j, $j = \overline{1, H}$.

Можно предположить, что степень субъективизма экспертно-аналитических оценок вероятностей, рассчитанных по (10), (11), ниже, чем оценок P_t, P_V, ранее полученных по (3), (6). Это следует из того, что сама процедура нахождения оценок P_t^*, P_V^* позволяет достаточно объективно выявить, детализировать и учесть причины и факторы, влияющие на возникновение угрозы *t* и формирование условий, определяющих возможность ее реализации.

IV Выводы

Анализ экономико-стоимостных соотношений в системе «атака-защита» при исследовании угроз НСД в ИС позволяет построить эвристические модели для оценивания вероятностей угроз и уязвимостей информационных ресурсов.

Использование в эвристических моделях безразмерных относительных показателей экономико-стоимостного описания системы «атака-защита» в форме оценок эффективности действий атакующей и защищающейся сторон упрощает вопросы практического применения предложенных моделей, в частности, устраняется необходимость прямого количественного измерения затрат и потерь и обеспечивается их шкалирование на основе экспертных сравнительных суждений методом парного сравнения.

*Литература: **1**. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. М.: Компания Ай Ти; ДМК Пресс, 2004. - 348 с. **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. –416 с. **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**.Гладыш С. Организационные и методологические аспекты экспертной оценки информационной безопасности информационно-телекоммуникационных систем.// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.// науково-техн. зб. – Київ, 2006. – Вип. 1(12). – с. 178-188. **6**. Архипов А. Е., Архипова С. А., Носок С. А. Технологии экспертного оценивания в задачах защиты информации. // Інформаційні технології та комп'ютерна інженерія. - 2005.- № 2.-с. 61-66. **7**. Гринберг А. С., Горбачев Н. Н., Тепляков А. А. Защита информационных ресурсов государственного управления. – М.: Юнити-ДАНА, 2003. – 327 с. **8**. Щеглов Ю. А. Защита компьютерной информации от несанкционированного доступа.- СПб: Наука и техника, 2004–384 с. **9.** Герасименко В. А. Защита информации в автоматизированных системах обработки данных. Кн. 1. – М.: Энергоатомиздат, 1994. – 400с. **10.** Андрощук Г. А., Крайнев П. П. Экономическая безопасность предприятия: защита коммерческой тайны. – К.: Изд. Дом «Ин Юре», 2000. – 400 с. **11.** Толстова Ю. Н. Измерение в социологии.- М.: ИНФРА – М, 1998. – 224 с.*