# Забезпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

**УДК 004.056**

## ПРИМЕНЕНИЕ СРЕДНЕГО РИСКА ДЛЯ ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

***Александр Архипов***

*Национальный технический университет Украины «Киевский политехнический институт»*

Анотації: **Розглянута можливість застосування теоретико-ймовірнісного апарату середніх ризиків для аналізу та оцінювання ефективності систем захисту інформації.**

Summary: **This paper considers an average risk probability-theoretic means that can be used for analysis and estimation efficiency of systems of information security.**

Ключові слова: **Середній ризик, системи захисту, ефективність, аудит безпеки, загроза, шкода.**

### I Введение

При организации режима информационной безопасности информационно-телекоммуникационной системы (ИТС) принципиально важным является наличие некоторого общего подхода, позволяющего, исходя из данных методологических предпосылок, решать всю совокупность задач, связанных с обеспечением информационной безопасности в ИТС. В частности, наличие подобного универсального методологического базиса позволяет осуществить логически увязанную последовательность действий по проектированию, разработке, реализации и сопровождению комплексной системы защиты информации (КСЗИ) в ИТС. В последнее время в качестве такого концептуального подхода предлагается использовать методологию анализа информационных рисков [1, 2], успешно применяемую как на этапе идентификации ключевых информационных ресурсов ИТС и оценивании их важности, так и при анализе уязвимостей информационной системы, оценивании угроз информации, при решении задачи выбора средств, методов и механизмов защиты, оценивании эффективности возможных вариантов КСЗИ. Основные положения методологии анализа информационных рисков, процедура её применения к разработке и построению КСЗИ, включая состав, последовательность и описание содержания выполняемых работ, достаточно полно освещены в специальной литературе [1 – 5].

При решении задач формально-расчетного обобщающего этапа анализа информационных рисков предполагается использование хорошо разработанного теоретико-вероятностного аппарата средних рисков [6 – 8], обеспечивающего получение строгих и математически обоснованных решений, приводящих в конечном итоге к построению корректных непротиворечивых расчетных методик. Однако именно здесь, в ходе адаптации имеющихся теоретических наработок к решению конкретных практических задач, возникают определенные трудности, анализ и преодоление которых является весьма актуальным.

### II Постановка задачи

В работе [1], авторы которой позиционируют её как "первое полное русскоязычное руководство по вопросам анализа информационных рисков и управления ими", базовым понятием является риск *r*, представляющий собой функцию вида:

$$r = p(t)\,q(t), \tag{1}$$

где $p(t)$ – вероятность реализации некоторой угрозы $t$ по отношению к конкретному информационному ресурсу $I$, а $q(t)$ – величина причиненного этой реализацией ущерба, называемая функцией потерь (штрафа) [8]. Расчетные соотношения для вычисления риска в более сложных ситуациях (например, при наличии нескольких угроз или большего числа информационных ресурсов) в [1 – 3] отсутствуют. Отмечается лишь, что при количественном задании исходных данных риск представляет собой математическое ожидание потерь [1]. Последняя формулировка является вербальным определением среднего риска [8] и удовлетворяет соотношению

$$R = \sum_{i=1}^{n} p(t_i)\, q(t_i), \tag{2}$$

в котором вероятности $p(t_i)$, $i = \overline{1,n}$ соответствуют вероятностям реализации отдельных событий, в совокупности составляющих полную систему (группу) [8]. Множество угроз $t = \{t_1,...,t_n\}$ в общем случае не образует полной системы, т. к. для угроз не являются обязательным требования попарной несовместности и полноты:

$$t_i \cap t_j \neq 0, \quad i \neq j, \quad t_i, t_j \in t, \quad \sum_{i=1}^{n} p(t_i) \neq 1, \tag{3}$$

поэтому выражение (2), составленное для угроз безопасности ИТС, в общем случае не определяет средний риск.

Выражение, аналогичное (2), приводится в [9], где называется общим риском. Там же, в выводах, как и в тексте [1], встречается выражение “суммарный риск”, в формульном представлении в этих источниках не описываемое. Поэтому возникает необходимость определиться с содержанием терминов, употребляемых при анализе информационных рисков, а также получить ряд соотношений, применимых при формализации описания методик оценивания информационных рисков.

## III Оценивание рисков атак

В общем случае событиями, результатом наступления которых оказывается реализация преднамеренных угроз безопасности ИТС, являются атаки, предпринимаемые в отношении некоторого информационного ресурса *I*. Поэтому анализ информационных рисков можно построить на анализе возможностей осуществления совокупности атак $A = \{a_1,...,a_N\}$ и сопряженных с их успешным завершением возможных потерь $q(a_k), k = \overline{1,N}$. Если известны вероятности успешного завершения атак, составляющие вектор $P_A = \{p(a_1),...,p(a_N)\}$, элементы которого зависят от наличия и характера уязвимостей ИТС, то, хотя множество $A$ и не образует полной группы событий, на его базе достаточно просто построить новое множество $\alpha = \{\alpha_1,...,\alpha_L\}$, удовлетворяющее требованиям полной группы. При этом в качестве элементов множества $\alpha$ будут фигурировать сложные события, представляющие собой совмещение $N$ событий из элементов множества $A = \{a_1,...,a_N\}$ и множества противоположных событий $A' = \{\bar{a}_1,...,\bar{a}_N\}$. Принципиальным при формировании множества событий $\alpha$ является требование введения в него всех возможных сочетаний элементов множества $A$, включая само множество $A$:

$$\alpha_1 = a_1 \cap a_2 \cap ... \cap a_N \tag{4}$$

и пустое множество атак, составленное из элементов множества $A'$:

$$\alpha_L = \bar{a}_1 \cap \bar{a}_2 \cap ... \cap \bar{a}_N. \tag{5}$$

Процедуру построения элементов $\alpha_j, j = \overline{1,L}$ можно представить рядом последовательных этапов:

1) формулирование упорядоченного множества возможных вариантов комплексных атак в виде соответствующих совокупностей элементов множества $A$, получаемых перебором всех возможных сочетаний $C_N^r, r = N, N-1,...,1,0$ элементов множества $A$ (например, при $N = 3$: $C_3^3 = a_1, a_2, a_3;\ C_3^2 = \{a_1, a_2; a_1, a_3; a_2, a_3\};\ C_3^1 = \{a_1; a_2; a_3\};\ C_3^0 = \emptyset$);

2) дополнение неполных совокупностей, т. е. содержащих менее $N$ элементов, до полных путем введения вместо недостающих элементов множества $A$ противоположных им элементов множества $A'$ (для данных примера n. 1):

$a_1, a_2, a_3; a_1, a_2, \bar{a}_3; a_1, \bar{a}_2, a_3; \bar{a}_1, a_2, a_3; a_1, \bar{a}_2, \bar{a}_3; \bar{a}_1, a_2, \bar{a}_3; \bar{a}_1, \bar{a}_2, a_3; \bar{a}_1, \bar{a}_2, \bar{a}_3$);

3) получение элементов $\alpha_j$ в виде пересечений (произведений) элементов соответствующих полных совокупностей ((для примера п. n. 1), 2): $\alpha_1 = a_1 \cap a_2 \cap a_3$; $\alpha_2 = a_1 \cap a_2 \cap \bar{a}_3$; $\alpha_3 = a_1 \cap \bar{a}_2 \cap a_3$;

$\alpha_4 = \bar{a}_1 \cap a_2 \cap a_3$; $\alpha_5 = a_1 \cap \bar{a}_2 \cap \bar{a}_3$; $\alpha_6 = \bar{a}_1 \cap a_2 \cap \bar{a}_3$; $\alpha_7 = \bar{a}_1 \cap \bar{a}_2 \cap a_3$; $\alpha_8 = \bar{a}_1 \cap \bar{a}_2 \cap \bar{a}_3)$.

Количество элементов множества $\alpha$ равно $L = 2^N$. Эти элементы представляют собой набор несовместных событий, позволяющих описать любую ситуацию (комплексную атаку), которая может возникнуть при произвольном сочетании атак из множества $A$. Чтобы определить риски событий $\alpha_j, j = \overline{1, L}$, необходимо задать распределение вероятностей этих событий и найти значения функции потерь для каждого из них, т. е. элементам множества $\alpha$ необходимо поставить в соответствие новый вектор $P_\alpha = \{p(\alpha_1),..., p(\alpha_L)\}$ и новые значения функции потерь $q(\alpha_j),\ j = \overline{1, L}$. Расчет этих характеристик осуществляется исходя из структуры соответствующих сложных событий $\alpha_j$. В частности, вероятность $p(\alpha_j)$ рассчитывается путем механической замены в структуре сложного события $\alpha_j$ элементов $a_k, k = \overline{1, N}$, принадлежащих множеству $A$, на вероятности $p(a_k)$ и, соответственно, элементов $\bar{a}_k$ на вероятности $1 - p(a_k)$ с последующим перемножением полученной последовательности из $N$ сомножителей. Например, для $\alpha_j = a_1 \cap \bar{a}_2 \cap \bar{a}_4 \cap ... \cap a_N$ получаем

$$p(\alpha_j) = p(a_1)(1 - p(a_2))(1 - p(a_3))...p(a_N). \quad (6)$$

Построение функций потерь для сложных событий обычно предваряется принятием гипотезы об аддитивности последствий атак, составляющих это сложное событие [6]. В этом случае определение значений функции потерь $q(\alpha_j)$ производится путем механической замены элементов $a_k$, $k = \overline{1, N}$ в структуре сложного события $\alpha_j$ значениями соответствующих потерь $q(a_k)$ и сложения полученной последовательности потерь (элементы $\bar{a}_k$ заменяются нулями). Для рассмотренного выше примера имеем

$$q(\alpha_j) = q(a_1) + ... + q(a_N). \quad (7)$$

Первый и последний элементы множества $\alpha$ характеризуются следующими параметрами:

$$p(\alpha_1) = \prod_{j=1}^{N} p(a_j), \quad q(\alpha_1) = \sum_{j=1}^{N} q(a_j), \quad (8)$$

$$p(\alpha_L) = \prod_{j=1}^{N} (1 - p(a_j)) = 1 - \sum_{j=1}^{N} p(a_j), \quad q(\alpha_L) = 0. \quad (9)$$

Определив все значения вероятностей $p(\alpha_j)$ и потерь $q(\alpha_j),\ j = \overline{1, L}$, рассчитываем средний риск, обусловленный множеством атак $A$ (или множеством комплексных атак $\alpha$), т. е. среднее значение возможного ущерба от атак $a_1, a_2, ..., a_N$, успешное завершение каждой из которых является случайным событием:

$$R_A = R_\alpha = \sum_{j=1}^{L-1} p(\alpha_j) q(\alpha_j). \quad (10)$$

Разработки КСЗИ для ИТС, в частности, принятие контрмер организационно-правового, программно-технического и инженерного характера позволяет снизить уровень рисков атак, уменьшив вероятности их успешного завершения до некоторых остаточных значений $p_o(a_k),\ k = \overline{1, N}$. Выбор лучшего варианта защиты можно осуществить, задавшись каким-либо критерием оценки эффективности КСЗИ [5]. Например, зная остаточные вероятности $p_o(a_k),\ k = \overline{1, N}$ для сопоставляемых вариантов, можно для каждого из них произвести расчет значений остаточных вероятностей сложных событий $p_o(\alpha_j)$ и затем по формуле (10) найти средний риск $R_{oA}$ по каждому варианту. Лучшей системе защиты будет

соответствовать минимальное значение среднего риска $R_{oA}$. Эффективность выбранного варианта защиты можно оценить по формуле

$$E = (R_A - R_{oA}) / R_A. \quad (11)$$

Значения $E$ могут лежать в диапазоне $0 \le E \le 1$, причем, чем выше эффективность системы защиты, тем ближе $E$ к единице. Показатель (11) ориентирован на оценивание защищенности стратегического информационного ресурса, для которого затраты на защиту носят второстепенный характер в силу того, что они намного меньше возможных потерь $R_A$. Учесть затраты, связанные с построением КСЗИ, позволяет показатель [10]

$$ROI = (R_A - R_{oA} - C) / C \quad (12)$$

– показатель возврата инвестиций (ROI – return of investment), C – общие затраты на создание и обслуживание КСЗИ, в англоязычной литературе – TCO (total cost of ownership). Если предотвращаемый вероятный ущерб $R_A - R_{oA}$ примерно равен затратам C, значение ROI близко к нулю, но стремительно возрастает, если затраты на безопасность $C << R_A - R_{oA}$.

В изложенном выше материале существенную смысловую нагрузку несёт понятие совместности событий [8] (в частности, атак), на физическом уровне иногда трактуемое как одновременность их протекания (развития) во времени. Подобное понимание является весьма суженным. Совместность атак – это возможность их реализации (но отнюдь не единовременная) относительно одного и того же ресурса в течение определенного промежутка времени, в продолжение которого потребительская стоимость ресурса, его полезность, эффективность целевого применения, а также связанные с этим возможные потери в случае успешного проведения атак остаются практически неизменными, стабильными.

Следует отметить, что принятие гипотезы аддитивности потерь при реализации некоторого сложного события тесно связано с введенным выше определением понятия одновременности событий (атак, угроз). В частности, если в некотором сложном событии, представляющем собой совмещение ряда атак, первой реализуется атака, приводящая к уничтожению информационного ресурса, то суммарный эффект от реализации всех последующих атак будет нулевым, в связи с тем, что исчезает сам объект атак и ущерб данного сложного события сводится к ущербу от потери информационного ресурса. Такое сложное событие не может рассматриваться как сочетание нескольких совместных, т. к. в процессе реализации этого события происходит изменение состояния информационного ресурса, выражающееся в изменении его стоимости (уменьшении ее до нуля) и соответствующем изменении значений возможных потерь. Следовательно, не выполняется ключевое для определения совместных событий требование стабильности свойств ресурса и значений возможных потерь. Однако, если результатом первой атаки будет нарушение конфиденциальности, влекущее за собой соответствующий ущерб, то сохраняется (как минимум до установления потерпевшей стороной факта нарушения конфиденциальности) аддитивность ущерба от возможной реализации других атак, входящих в рассматриваемое сложное событие.

## IV Оценивание рисков на уровне угроз

Анализ рисков на уровне атак позволяет, по-видимому, наиболее объективно проанализировать и учесть реальную ситуацию с безопасностью ИТС. Однако это требует задания максимально полной и детализированной информации об уязвимостях ИТС, непосредственно являющихся объектами атак, а, следовательно, проведения тщательного и квалифицированного аудита безопасности ИТС, позволяющего учесть индивидуальные бреши в аппаратно-программном обеспечении и защите ИТС. При этом объем сведений о возможных атаках может стать достаточно большим, что из-за экспоненциального характера зависимости числа $L$ сложных событий, составляющих множество $\alpha$, от числа атак $N$ приведет к крайней громоздкости и трудоемкости процедуры вычисления и анализа информационных рисков атак (даже если учесть, что часть событий множества $\alpha$ придется исключить из-за нереальности представляемых ими комплексных атак). В этой ситуации, учитывая, что большая часть сведений, используемых для анализа рисков атак, добыта экспертным путем, целесообразно попытаться укрупнить получаемые экспертные оценки до уровня анализа угроз (вероятностей реализации угроз, возможных потерь от реализации угроз).

Предположим, исследование исходного множества атак $A$ позволило разделить их на ряд непересекающихся подмножеств $A_1,...,A_i,...,A_n$ с объемами $N_1,...,N_i,...,N_n$ в соответствии с

основными типами угроз $t_1,...,t_i,...,t_n$ (конфиденциальности, доступности и т. п. [11]). Очевидно, что осуществление любой из атак, входящей в соответствующее подмножество $A_i$, относительно одного и того же информационного ресурса *I*, повлечет одинаковые потери $q(t_i),\ i=\overline{1,n}$. В этом случае возможно проведение предварительного оценивания вероятностей реализации угроз, составляющих множество $t=\{t_1,...,t_n\}$ с последующим использованием этих данных в расчете среднего риска безопасности ТКС. Для определения угрозы $t_i,\ i=\overline{1,n}$, реализация которой зависит от успешности атак, составляющих множество $A_i$, имеем:

$$p(t_i)=1-\prod_{a_g\in A_i}(1-p(a_g)). \tag{13}$$

Как отмечалось при постановке задачи, множество угроз $t$ не составляет полной группы событий. Поэтому так, как это было сделано выше для множества атак $A$, из элементов множества $t$ строим совокупность вариантов комплексных угроз в виде всех возможных сочетаний элементов множества угроз $C_n^r, r=n,n-1,...,1,0$, дополняем число элементов в каждом полученном сочетании до $n$ путем введения вместо недостающих элементов множества $t$ противоположных им элементов из множества $t'$ и формируем из полученных наборов элементов их пересечения, каждому из которых соответствует элемент множества $T$. Совокупность из $M=2^n$ элементов множества $T$ представляет полную группу:

$$T_i\cap T_j=0,\ \ i\neq j,\quad T_i,T_j\in T,\quad \sum_{j=1}^{M}p(T_j)=1. \tag{14}$$

Потери $q(T_j), j=\overline{1,M}$, в предположении аддитивности потерь от одновременно реализуемых угроз, определяются в соответствии с процедурой, введенной ранее для оценивания значений функции потерь $q(\alpha_i)$ (пример, иллюстрирующий получение расчетных соотношений, представлен выражениями (7) – (9)). Учитывая, что элементу $T_M$ соответствует пустое множество угроз $T_M=\bar{t}_1\cap\bar{t}_2\cap...\cap\bar{t}_n$, для которого $q(T_M)=0$, получаем формулу среднего риска угроз:

$$R_T=R_t=\sum_{j=1}^{M-1}p(T_j)q(T_j), \tag{15}$$

по виду практически аналогичную ранее полученному соотношению (10) для среднего риска атак. Так же, как и последний, средний риск $R_t$ применим для выбора вариантов защиты, оценивания эффективности КСЗИ.

## V Анализ рисков при множестве защищаемых ресурсов

Если отдельные составляющие общего информационного ресурса $\mathrm{I}=\{\mathrm{I}_1,...,\mathrm{I}_m\}$ отличаются по уровню своей важности, режиму доступа и т. п., возникает необходимость в раздельном учете и влиянии угроз (атак) на эти составляющие. В таком случае для анализа возможных ситуаций, соответствующих различным объемам атакуемых ресурсов, различиям в уровнях комплексирования угроз (атак), целесообразно ввести в рассмотрение матрицу–индикатор угроз (атак) размерностью $m\times n$, число строк $m$ которой соответствует числу защищаемых ресурсов, а количество столбцов $n$ – количеству угроз (атак). Если реализация *i*-ой угрозы (атаки) представляет опасность для *r*-ого ресурса, то на пересечении *i*-ого столбца и *r*-ной строки ставится единица, при отсутствии опасности – 0. Ниже приведен пример такой матрицы, называемой также матрицей инцидентности:

$$E=\begin{bmatrix}1&0&0&1&...&1\\0&1&0&1&...&0\\-&-&-&-&-&-\\1&0&1&1&...&1\end{bmatrix}, \tag{16}$$

заполнение которой требует максимального объема сведений о характере информационных ресурсов и свойствах угроз (атак). Наличие сведений о количественных значениях потерь, обусловленных реализацией тех или иных угроз (атак) относительно конкретных информационных ресурсов, позволяет из матрицы $E$ путем замены единиц на соответствующие значения потерь получить матрицу потерь $[q_{ri}]$, а при наличии данных о вероятностях этих потерь – матрицу вероятностей $[p_{ri}]$.

Для конкретизации и упрощения последующего анализа ограничимся рассмотрением случая воздействия множества атак $A=[a_1,...,a_n]$ на некоторый общий ресурс $I$, содержащий три составляющие: $I_1$ – информационный ресурс, объединяющий сведения особой важности, $I_2$ – совершенно секретные сведения, $I_3$ – секретные сведения. Исходные данные для этого случая представлены в таблице

| $I$ | $A$ | | | |
|---|---|---|---|---|
| | $a_1$ | $a_2$ | .... | $a_n$ |
| $I_1$ | $q_{11}, p_{11}$ | $q_{12}, p_{12}$ | .... | $q_{1n}, p_{1n}$ |
| $I_2$ | $q_{21}, p_{21}$ | $q_{22}, p_{22}$ | .... | $q_{2n}, p_{2n}$ |
| $I_3$ | $q_{31}, p_{31}$ | $q_{32}, p_{32}$ | .... | $q_{3n}, p_{3n}$ |

Центральная часть таблицы образует матрицу $[q_{ri}, p_{ri}]$, полученную попарным объединением соответствующих элементов матриц потерь и вероятностей.

Очевидно, что воздействию атак могут подвергаться как отдельные информационные ресурсы $I_1$, $I_2$, $I_3$, так и их сочетания, при этом сами атаки могут иметь комплексный характер, т. е. одновременно будет осуществляться несколько атак. Для применения методологии средних рисков необходимо выполнить трансформацию множества атак $A$ в составляющее полную группу событий множество $\alpha$ (как это уже делалось выше в третьем разделе), а также преобразовать множество $I$ в множество событий $I=\{I_1,...,I_8\}$, удовлетворяющих требованиям к полной группе.

В соответствие с описанной выше процедурой построения этих событий имеем: $I_1=I_1\cap I_2\cap I_3$, $I_2=I_1\cap I_2\cap \bar{I}_3$, $I_3=I_1\cap \bar{I}_2\cap \bar{I}_3$, …, $I_7=\bar{I}_1\cap \bar{I}_2\cap I_3$, $I_8=I_1\cap \bar{I}_2\cap \bar{I}_3$. В соответствии со структурой выражений, полученных для событий $I_l$, $l=\overline{1,8}$, предполагая выполняющейся гипотезу аддитивности потерь, отдельно для каждого *i*-ого столбца рассчитываем значения потерь $q^*_{li}$ и их вероятностей $p^*_{li}$: $q^*_{1i}=q_{1i}+q_{2i}+q_{3i}$, $q^*_{2i}=q_{1i}+q_{2i}$, $q^*_{3i}=q_{1i}+q_{3i}$, …, $q^*_{7i}=q_3$, $q^*_{8i}=0$, соответственно, $p^*_{1i}=p_{1i}\,p_{2i}\,p_{3i}$, $p^*_{2i}=p_{1i}\,p_{2i}\,(1-p_{3i})$, $p^*_{3i}=p_{1i}(1-p_{2i})\,p_{3i}$, …, $p^*_{7i}=(1-p_{1i})(1-p_{2i})\,p_{3i}$, $p^*_{8i}=1-\sum_{l=1}^{7}p^*_{li}$.

Выполнив эту группу преобразований, получаем некоторую переходную (промежуточную) матрицу $[q^*_{li}, p^*_{li}]$ размерностью $8\times n$, в которой учтены возможные последствия воздействия отдельных атак $a_i$, $i=\overline{1,n}$ одновременно на несколько информационных ресурсов.

Далее необходимо сформировать элементы множества $\alpha$ (что уже рассматривалось ранее) и, с учетом их структур, по каждой отдельной $l$-ой строке матрицы $[q^*_{li}, p^*_{li}]$ выполнить расчеты потерь $Q_{lj}$ и вероятностей $P_{lj}$ для соответствующих элементов $\alpha_j$, $j=\overline{1,M}, M=2^n$. Следует отметить, что элементу $\alpha_M$ соответствует событие $\bar{a}_1\cap\bar{a}_2\cap...\cap\bar{a}_n$, соответствующее отсутствию атак, поэтому для

правого столбца матрицы $[Q_{lj}, P_{lj}]$ получаем: $Q_{lM} = 0,\ l = \overline{1,8}$. Аналогичная ситуация имеет место для нижней строки этой матрицы, $Q_{8j} = 0$, $j = \overline{1,M}$, т.к. событие $I_8 = \bar{I}_1 \cap \bar{I}_2 \cap \bar{I}_3$ соответствуем пустому множеству ресурсов. С учетом этого получаем выражение для среднего риска потерь от воздействия множества атак на множество информационных ресурсов:

$$R(A, I) = \sum_{j=1}^{M-1} \sum_{l=1}^{G-1} Q_{lj} P_{lj}, \tag{17}$$

где $G = 2^m$ – количество событий в множестве $I$ в общем случае, когда множество $I$ состоит из $m$ элементов. Анализируя степень существенности различных вариантов атак можно подсчитать риски потерь от комплексных атак, определив соответствующее событие $\alpha_j$, в структуру которого входит данная комплексная атака:

$$R(\alpha_j, I) = \sum_{l=1}^{G-1} Q_{lj} P_{lj}, \tag{18}$$

Можно оценить уровень потерь от возможных вариантов атак отдельного информационного ресурса или группы ресурсов, выбрав предварительно событие $I_l$, в структуре которого представлен отдельный ресурс либо их группа:

$$R(A, I_l) = \sum_{j=1}^{M-1} Q_{lj} P_{lj}, \tag{19}$$

Наконец, оценка вероятных потерь от некоторой атаки (комплекса атак), представленной в структуре события $\alpha_j$, на группу информационных ресурсов, которой соответствует структура элемента $I_l$, определяется частным риском

$$R(\alpha_l, I_l) = Q_{lj} P_{lj}. \tag{20}$$

Очевидно, что располагая информацией о значениях остаточных вероятностей $[p_{ori}]$, получаемых при оценке того или иного варианта защиты, можно подсчитать соответствующие остаточные риски и выбрать наиболее подходящий вариант защиты.

Приведенные выше в общем виде выкладки выглядят довольно громоздкими. На практике, учитывая, что в матрице-индикаторе $E$ вероятно наличие определенного количества нулей, размерность множеств $\alpha$ и $I$ может существенно понизиться за счет исключения из них ряда формально вводимых событий, вероятность которых окажется равной 0. Упрощения решаемой задачи иногда можно достичь за счет перехода от анализа атак к анализу угроз, т. к. при этом возможно сокращение числа столбцов матрицы $E$. При этом очевидно, что сам процесс анализа потерь и рисков, как и полученные соотношения (17) – (20), не изменятся при формальной замене множества атак $A$ множеством угроз $t$.

Иногда на начальных этапах анализа угроз целесообразным оказывается применение упрощенных или приближенных процедур анализа. Например, если известна только матрица потерь $[q_{ri}]$, произведение

$$e[q_{ri}] = Q(t) = [Q(t_1), ..., Q(t_n)], \tag{21}$$

где $e_m = [1,1,...,1]$ – единичная вектор-строка, состоящая из $m$ единиц, позволяет рассчитать вектор-строку "полных" потерь в результате реализации соответствующих составляющих вектора угроз $t = [t_1, ..., t_n]$,

$$Q(t_i) = \sum_{r=1}^{m} q_{ri}, i = \overline{1,n}. \tag{22}$$

Знание количественных значений оценок элементов $Q(t_i),\ i = \overline{1,n}$ позволяет приближенно оценить значимость различных угроз, выполнить их ранжирование, приступить к нейтрализации наиболее существенных угроз. Если в (21) вместо матрицы $[q_{ri}]$ использовать матрицу $[q_{ri}, p_{ri}]$, составленную из парных произведений соответствующих элементов матриц $[q_{ri}]$, $[p_{ri}]$, то получим вектор-строку

взвешенных потерь, рассчитанную с учетом вероятностей возникновения частных потерь $p_i$. Для угроз $t_i$ сопоставление величин взвешенных потерь

$$Q\ (t_i) = \sum_{r=1}^{m} q_{ri}\ p_{ri},\ i = \overline{1,n} \tag{23}$$

может привести к результатам ранжировки угроз, несколько отличным от ранее полученных. Однако взвешивание потерь по их вероятности позволяет более объективно оценить эффективность применяемых средств и методов защиты, проанализировать и сравнить возможные варианты контрмер. Для этого необходимо располагать сведениями об остаточных вероятностях потерь $[p_{ori}]$, зная которые можно по аналогии с выражением (23) рассчитать взвешенные остаточные потери $Q_o^*(t) = [\,Q_o^*(t_1),...,Q_o^*(t_n)]$.

На практике возможно возникновение различных ситуаций, допускающих упрощение условий исходной постановки общей задачи, комбинированное применение к её решению уже рассмотренных выше процедур и вариантов обработки данных, позволяющих корректно провести анализ информационных рисков.

## VI Выводы

Предложена методика применения теоретико-вероятностного аппарата средних рисков для решения задач анализа и оценивания эффективности систем защиты информации. Разработана процедура преобразования исходных данных, получаемых при проведении аудита информационных систем, к виду, допускающему непосредственное вычисление функционала среднего риска. Получены основные расчетные соотношения. Приведены некоторые упрощенные варианты анализа эффективности систем защиты.

*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**. Астахов А. М. Аудит безопасности ИС // Конфидент. Защита информации. - №1. – 2003. – с. 63 – 67. **5**. Архипов О. Є., Ворожко В. П. Системний підхід до оцінювання ефективності захисту державної таємниці // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні// науково-техн. зб. – Київ, 2005. – Вип. 10. – с.18 – 22. **6**. Качинський А. Б. Безпеки, загрози і ризик: Наукові концепції та математичні методи. - К.: 2003.- 472 с. **7**. Алгоритмы и программы восстановления зависимостей / Под ред. В. Н. Вапника. – М.: Наука, 1984. – 816 с. **8**. Пугачев В. С. Теория вероятности и математическая статистика. – М.: Наука, 1979. – 496 с. **9.** Воробиенко П., Нечипорук О., Щербина Ю. Принципы построения модели угроз информационным ресурсам систем и сетей связи // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Вип. 7 – К.: 2003. - с. 11 – 13. **10.** Гостев И. М. Безопасность – бесполезная трата денег или их выгодное вложение?// Конфидент. Защита информации. - №5. – 2003. – с. 16 – 18. **11.** НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.*

**УДК 681.3.06**

# МЕТОД ПОБУДОВИ S-БЛОКІВ З ВЛАСТИВІСТЮ КОРЕЛЯЦІЙНОЇ ІМУННОСТІ КООРДИНАТНИХ ФУНКЦІЙ

***Олександр Дирда, Леонід Скрипник***

*Інститут спеціального зв'язку та захисту інформації НТУУ "КПІ"*

Анотація: **Розглядаються методи побудови кореляційно-імунних булевих функцій та еластичних функцій для синтеза криптографічних алгоритмів. Запропоновано евристичний алгоритм побудови збалансованої кореляційно-імунної функції, а також метод побудови S-блоків з властивістю кореляційної імунності першого порядку координатних функцій.**

Summary: **Methods of construction of correlative-immune Boolean functions and resilient functions for synthesis of cryptographic algorithms are regarded. It is proposed heuristic algorithm of construction of balanced correlative-immune function, and also are proposed methods of construction of S-blocks with**