DOI: **10.18372/2410-7840.18.11091**
УДК 004.056.5(045)

БИСТАБИЛЬНАЯ ИНТЕГРИРОВАННАЯ КОРТЕЖНАЯ МОДЕЛЬ ХАРАКТЕРИСТИК РИСКА

Александр Корченко, Светлана Казмирчук, Юрий Дрейс, Андрей Гололобов

Часто перед специалистами соответствующих компаний для повышения эффективности решения задач защиты информации возникает вопрос о выборе существующих или разработке новых средств оценивания рисков безопасности ресурсов информационных систем. Для эффективной организации соответствующего процесса выбора или разработки необходимо иметь достаточно полное отображение характеристик риска. В связи с этим, в работе определены множества базовых характеристик риска для области информационной безопасности. На основании этого предлагается отображать заданные идентифицирующие и оценочные характеристики в виде бистабильной (бификсированной) интегрированной кортежной модели. На практике такую модель предлагается использовать в виде отображения на два частных кортежа – аналитический и синтетический, применяемые соответственно для реализации выбора существующих средств и для помощи разработчикам при создании новых систем оценивания рисков.

Ключевые слова: *анализ риска, оценивание риска, базовые характеристики риска, бистабильная интегрированная кортежная модель, частное отображение кортежа, риск информационной безопасности, лингвистическая переменная.*

Развитие IT-инфраструктуры предприятий влечет за собой стремительный неконтролируемый рост количества уязвимостей ресурсов информационных систем (РИС) [2, 16]. Для обеспечения необходимого уровня безопасности РИС обычно на предприятиях внедряют соответствующие системы защиты информации (ЗИ) [2, 6, 16]. Одним из основных этапов построения таких систем является реализация процесса анализа и оценивания рисков информационной безопасности (ИБ). На сегодняшний день существует множество инструментальных средств [6], которые объединяются в методики оценивания и анализа рисков. Часто перед специалистами в области ИБ возникает вопрос об эффективном выборе существующих или разработке новых средств оценивании состояния безопасности РИС. Для эффективной организации соответствующего процесса выбора или разработки необходимо иметь достаточно полное отображение характеристик риска, связанных с ИБ.

В работе [6, 7] была разработана интегрированная модель представления параметров риска на основе десятикомпонентного кортежа, с помощью которой осуществлялся анализ подобных средств. При практическом использовании представленной в [6, 7] модели появилась необходимость в разделении входящих в нее параметров на те, посредством которых проводился бы анализ существующих средств оценивания и те, с помощью которых в перспективе в определенных условиях реализовывался процесс оценивании, например, в реальном времени или в условиях, позволяющих адаптировать нечеткие шкалы и др. В связи с этим, актуальной является задача определения характеристик риска, используемых для последующего выбора соответствующих средств, а также для синтеза новых систем оценивания рисков безопасности РИС. Последние, например, можно использовать для определения необходимого уровня ЗИ, осуществления его поддержки и разработки стратегии развития информационных систем (ИС) [2, 6, 16] с учетом постоянного роста количества уязвимостей ее ресурсов.

В связи с этим целью данной работы является усовершенствование известной интегрированной кортежной модели за счет введения множеств соответствующих характеристик риска и ее представления в виде отображения на два частных кортежа – аналитический и синтетический, применяемые соответственно для реализации выбора существующих средств и для помощи разработчикам при создании новых систем оценивания рисков безопасности РИС.

С целью формализации процесса формирования необходимых характеристик риска предлагается так называемая бистабильная интегрированная кортежная модель характеристик риска (БИМ) или аналитико-синтетическая кортежная модель характеристик риска (АСМ) (см. рис. 1). С ее помощью для достижения цели исследований

осуществляется формирование требуемых аналитического и синтетического кортежей. Для этого введем множество всех возможных характеристик риска:

$$\boldsymbol{BC} = \{\bigcup_{i=1}^{bc} \boldsymbol{BC}_i\} = \{\boldsymbol{BC}_1, \boldsymbol{BC}_2, ..., \boldsymbol{BC}_{bc}\}, \quad (1)$$

где $\boldsymbol{BC}_i \subseteq \boldsymbol{BC}$ $(i = \overline{1, bc})$ – подмножество отображаемое i-ю характеристику риска. Это подмножество можем представить, в следующем виде:

$$\boldsymbol{BC}_i = \{\bigcup_{bo=1}^{n_i} BC_{i,bo}\} = \{BC_{i,1}, BC_{i,2}, ..., BC_{i,n_i}\} \quad (2)$$

Таким образом, (1) с учетом (2) можем записать как:

$$\begin{aligned} &\{\bigcup_{i=1}^{bc} \boldsymbol{BC}_i\} = \{\bigcup_{i=1}^{bc} \{\bigcup_{bo=1}^{n_i} BC_{i,bo}\}\} = \\ &\{\bigcup_{i=1}^{bc} \{BC_{i,1}, BC_{i,2}, ..., BC_{i,n_i}\}\} = \\ &\{\{BC_{1,1}, BC_{1,2}, ..., BC_{1,n_1}\}, \\ &\{BC_{2,1}, BC_{2,2}, ..., BC_{2,n_2}\}, ..., \\ &\{BC_{bc,1}, BC_{bc,2}, ..., BC_{bc,n_{bc}}\}\}, \end{aligned} \quad (3)$$

где bc и n_i – соответственно количество членов в $\boldsymbol{BC}$ и $\boldsymbol{BC}_i$, $(i = \overline{1, bc},\ bo = \overline{1, n_i})$.

Например, с учетом (1)–(3) при bc=13, $n_1 = aes = n_2 = ca = n_3 = cs = n_{11} = sc = n_{13} = va =$ 2, $n_4 = d = n_5 = dt = n_7 = f = n_9 = me = n_{10} = p =$ $n_{12} = n$ =3, $n_6 = e$ = 7 и $n_8 = l$ = 5 множество $\boldsymbol{BC}$ имеет следующий вид [1, 3, 8-11, 13-15]: $\{\bigcup_{i=1}^{13} \boldsymbol{BC}_i\} = \{\bigcup_{i=1}^{13} \{\bigcup_{bo=1}^{n_i} BC_{i,bo}\}\} = \{\{BC_{1,1}, BC_{1,2}\}$, $\{BC_{2,1}, BC_{2,2}\}$, $\{BC_{3,1}, BC_{3,2}\}$, $\{BC_{4,1}, BC_{4,2}, BC_{4,3}\}$, $\{BC_{5,1}, BC_{5,2}, BC_{5,3}\}$, $\{BC_{6,1}, BC_{6,2}, BC_{6,3}, BC_{6,4}, BC_{6,5}, BC_{6,6}, BC_{6,7}\}$, $\{BC_{7,1}, BC_{7,2}, BC_{7,3}\}$, $\{BC_{8,1}, BC_{8,2}, BC_{8,3}, BC_{8,4}, BC_{8,5}\}$, $\{BC_{9,1}, BC_{9,2}, BC_{9,3}\}$, $\{BC_{10,1}, BC_{10,2}, BC_{10,3}\}$, $\{BC_{11,1}, BC_{11,2}\}$, $\{BC_{12,1}, BC_{12,2}, BC_{12,3}\}$, $\{BC_{13,1}, BC_{13,2}\}\} = \{\{AES_1, AES_2\}, \{CA_1, CA_2\}, \{CS_1, CS_2\}, \{D_1, D_2, D_3\}, \{DT_1, DT_2, DT_3\}, \{E_1, E_2, E_3, E_4, E_5, E_6, E_7\}, \{F_1, F_2, F_3\}, \{L_1, L_2, L_3, L_4, L_5\}, \{M_1, M_2, M_3\}, \{P_1, P_2, P_3\}, \{SC_1, SC_2\}, \{V_1, V_2, V_3\}, \{VA_1, VA_2\}\}$.

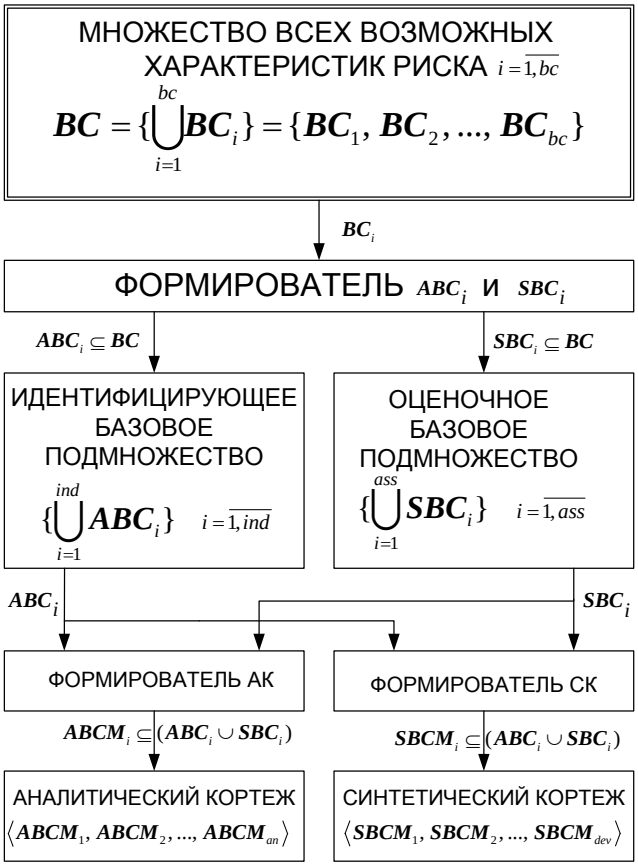

Рис. 1. Структурно-аналитическое отображение БИМ (АСМ)

Здесь в составе множества $\boldsymbol{BC}$ есть:

– элемент $\boldsymbol{AES}$ – **«Адаптивность нечетких шкал оценивания»** ($\boldsymbol{BC}_1 = \boldsymbol{AES}$), который может быть представлен в виде подмножества

$$\boldsymbol{BC}_1 = \{\bigcup_{bo=1}^{n_1} BC_{1,bo}\} = \boldsymbol{AES} = \{\bigcup_{bo=1}^{aes} AES_{bo}\},$$
$$(\boldsymbol{BC}_1 \subseteq \boldsymbol{BC},\ bo = \overline{1, aes}),$$

где $n_1 = aes$ – количество вариантов адаптируемости нечетких шкал оценивания, например, при aes =2 $\boldsymbol{BC}_1 = \{\bigcup_{bo=1}^{n_1} BC_{1,bo}\} = \{BC_{1,1}, BC_{1,2}\} = \boldsymbol{AES} = \{\bigcup_{bo=1}^{2} AES_{bo}\} = \{AES_1, AES_2\}$ = {«декрементирование», «инкрементирование»}, ($BC_{1,1} = AES_1$, $BC_{1,2} = AES_2$ – варианты адаптируемости нечетких шкал оценивания для параметрических нечетких чисел (НЧ), например, трапециевидных и треугольных). Этот элемент отражает возможности системы по трансформированию эталонов параметров и адаптации системы под разные условия среды оценивания без участия экспертов соответствующей предметной области;

– элемент CA – **«Калькулятор»** ($BC_2 = CA$), который может отражаться в виде подмножества $\boldsymbol{BC}_2 = \{\bigcup_{bo=1}^{n_2} BC_{2,bo}\} = \boldsymbol{CA} = \{\bigcup_{bo=1}^{ca} CA_{bo}\}$ ($\boldsymbol{BC}_2 \subseteq \boldsymbol{BC}$, $bo = \overline{1, ca}$), где $n_2 = ca$ – количество вариантов калькулятора, например, при ca=2 $\boldsymbol{BC}_2 = \{\bigcup_{bo=1}^{n_2} BC_{2,bo}\} = \{BC_{2,1}, BC_{2,2}\} = \boldsymbol{CA} = \{\bigcup_{bo=1}^{2} CA_{bo}\} = \{CA_1, CA_2\} =$ {«CVSS-калькулятор», «Риск-калькулятор»}, ($BC_{2,1} = CA_1$, $BC_{2,2} = CA_2$ – варианты калькулятора для оценивания риска и оценок CVSS). Этот элемент показывает наличие в системе возможности использования калькуляторов для оценивания риска, а также оценок CVSS;

– элемент CS – «**Характеристика ситуации**» ($BC_3 = CS$), который можно определить как подмножество $\boldsymbol{BC}_3 = \{\bigcup_{bo=1}^{n_3} BC_{3,bo}\} = \boldsymbol{CS} = \{\bigcup_{bo=1}^{cs} CS_{bo}\}$, ($\boldsymbol{BC}_3 \subseteq \boldsymbol{BC}$, $bo = \overline{1, cs}$), где $n_3 = cs$ – количество идентификаторов характеристики ситуации. Например, при cs=2 подмножество $\boldsymbol{BC}_3$ может представляться как: $\boldsymbol{BC}_3 = \{\bigcup_{bo=1}^{2} BC_{3,bo}\} = \{BC_{3,1}, BC_{3,2}\} = \boldsymbol{CS} = \{\bigcup_{bo=1}^{2} CS_{bo}\} = \{CS_1, CS_2\} =$ {«Определённая», «Нечеткая»}, где $BC_{3,1} = CS_1$, $BC_{3,2} = CS_2$ – элементы подмножества $\boldsymbol{CS}$, отображающие характеристику ситуации в виде лингвистических значений;

– элемент D – «**Опасность**» ($BC_4 = D$), который может отражаться посредством лингвистической переменной (ЛП) [4-7] $\boldsymbol{BC}_4 = \{\bigcup_{bo=1}^{n_4} BC_{4,bo}\} = \boldsymbol{D} = \{\bigcup_{bo=1}^{d} \underset{\sim}{D}_{bo}\}$, ($\boldsymbol{BC}_4 \subseteq \boldsymbol{BC}$, $bo = \overline{1, d}$), где $n_4 = d$ – количество термов ЛП «ОПАСНОСТЬ». Например, при d=3 подмножество $\boldsymbol{BC}_4$ может представляться как: $\boldsymbol{BC}_4 = \{\bigcup_{bo=1}^{n_4} \boldsymbol{BC}_{4,bo}\} = \{BC_{4,1}, BC_{4,2}, BC_{4,3}\} = \boldsymbol{D} = \{\bigcup_{bo=1}^{3} \underset{\sim}{D}_{bo}\} = \{\underset{\sim}{D}_1, \underset{\sim}{D}_2, \underset{\sim}{D}_3\} = \{\underset{\sim}{H}, \underset{\sim}{C}, \underset{\sim}{B}\}$, и отображаться НЧ $\underset{\sim}{H}$, $\underset{\sim}{C}$ и $\underset{\sim}{B}$, имеющими лингвистический эквивалент «низкая» (Н), «средняя» (С) и «высокая» (В) соответственно, где $BC_{4,1} = \underset{\sim}{D}_1$, $BC_{4,2} = \underset{\sim}{D}_2$, $BC_{4,3} = \underset{\sim}{D}_3$ – элементы базового терм-множества $\boldsymbol{D}$, отображающие значения опасности в виде НЧ;

– элемент DT – «**Отклонение от цели**» ($BC_5 = DT$), который является характеристикой, отображаемой численно (например, как стандартное (квадратичное), вероятное или допускаемое отклонение [6, 7]) или посредством применения логико-лингвистического подхода с помощью ЛП «ОТКЛОНЕНИЕ ОТ ЦЕЛИ», т.е.

$$\boldsymbol{BC}_5 = \{\bigcup_{bo=1}^{n_5} BC_{5,bo}\} = \boldsymbol{DT} = \{\bigcup_{bo=1}^{dt} \underset{\sim}{DT}_{bo}\}$$

$$(\boldsymbol{BC}_5 \subseteq \boldsymbol{BC}, \text{ а } \underset{\sim}{DT}_1 < \underset{\sim}{DT}_2 < \ldots < \underset{\sim}{DT}_{dt}, bo = \overline{1, dt})$$

,

где $n_5 = dt$ – количество термов ЛП «ОТКЛОНЕНИЕ ОТ ЦЕЛИ». Например, при dt=3 можно сформировать следующее множество термов: $\boldsymbol{BC}_5 = \{\bigcup_{bo=1}^{n_5} BC_{5,bo}\} = \{BC_{5,1}, BC_{5,2}, BC_{5,3}\} = \boldsymbol{DT} = \{\bigcup_{bo=1}^{3} \underset{\sim}{DT}_{bo}\} = \{\underset{\sim}{DT}_1, \underset{\sim}{DT}_2, \underset{\sim}{DT}_3\} =$ т{«Маленькое (М)», «Среднее (С)», «Большое (Б)»}, где $BC_{5,1} = \underset{\sim}{DT}_1$, $BC_{5,2} = \underset{\sim}{DT}_2$ и $BC_{5,3} = \underset{\sim}{DT}_3$ – элементы базового терм-множества $\boldsymbol{DT}$ отображающие значения отклонения от цели в виде НЧ $\underset{\sim}{M}$, $\underset{\sim}{C}$ и $\underset{\sim}{Б}$;

– элемент E – «**Нарушение базовых характеристик ИБ**» ($BC_6 = E$), который можно отобразить в виде символьной переменной, принимающей одно из значений конечного подмножества идентификаторов $\boldsymbol{BC}_6 = \{\bigcup_{bo=1}^{n_6} BC_{6,bo}\} = \boldsymbol{E} = \{\bigcup_{bo=1}^{e} E_{bo}\}$, ($\boldsymbol{BC}_6 \subseteq \boldsymbol{BC}, bo = \overline{1, e}$), где $n_6 = e$ – количество идентификаторов нарушения ИБ РИС. Например, при e=7 подмножество $\boldsymbol{BC}_6$ может представляться как: $\boldsymbol{BC}_6 = \{\bigcup_{bo=1}^{7} BC_{6,bo}\} = \{BC_{6,1}, BC_{6,2},$

$..., BC_{6,7}\} = \boldsymbol{E} = \{\bigcup_{bo=1}^{7} E_{bo}\} = \{E_1, E_2, ..., E_7\} =$ {«Нарушение конфиденциальности (НК)», «Нарушение целостности (НЦ)», «Нарушение доступности (НД)», «Нарушение целостности и конфиденциальности (НЦК)», «Нарушение целостности и доступности (НЦД)», «Нарушение конфиденциальности и доступности (НКД)», «Нарушение конфиденциальности, целостности и доступности (НКЦД)»}, где $BC_{6,1} = E_1$, $BC_{6,2} = E_2$, …, $BC_{6,7} = E_7$ – элементы подмножества $\boldsymbol{E}$, отображающие возможные варианты нарушения базовых характеристик ИБ РИС;

– элемент $\boldsymbol{F}$ – «**Частота**» ($\boldsymbol{BC}_7 = \boldsymbol{F}$), который аналогично $\boldsymbol{D}$ может определятся ЛП «ЧАСТОТА», например, при f=3 она имеет вид: $\boldsymbol{BC}_7 = \{\bigcup_{bo=1}^{n_7} BC_{7,bo}\} = \{BC_{7,1}, BC_{7,2}, BC_{7,3}\} = \boldsymbol{F} = \{\bigcup_{bo=1}^{f} \underset{\sim}{F}_{bo}\} = \{\bigcup_{bo=1}^{3} \underset{\sim}{F}_{bo}\} = \{\underset{\sim}{F}_1, \underset{\sim}{F}_2, \underset{\sim}{F}_3\}$ ($\boldsymbol{BC}_7 \subseteq \boldsymbol{BC}$, $bo = \overline{1, f}$), где $n_7 = f$ – количество термов ЛП «ЧАСТОТА» ($BC_{7,1} = \underset{\sim}{F}_1$, $BC_{7,2} = \underset{\sim}{F}_2$, $BC_{7,3} = \underset{\sim}{F}_3$ – элементы базового терм-множества $\boldsymbol{F}$, отображающие частоту в виде нечетких значений);

– элемент $\boldsymbol{L}$ – «**Расходы**» ($\boldsymbol{BC}_8 = \boldsymbol{L}$), который может быть представлен числено, например, на заданных интервалах 1) 0 – \$100; 2) \$100 – \$1000; 3) \$1000 – \$10 000; 4) \$10 000 – \$100 000. Здесь (по аналогии с $\boldsymbol{D}$) можно определить ЛП «РАСХОДЫ», например, $\boldsymbol{BC}_8 = \{\bigcup_{bo=1}^{n_8} BC_{8,bo}\} = \boldsymbol{L} = \{\bigcup_{bo=1}^{l} \underset{\sim}{L}_{bo}\}$, ($\boldsymbol{BC}_8 \subseteq \boldsymbol{BC}$, $bo = \overline{1, l}$), где $n_8 = l$ – количество термов ЛП «РАСХОДЫ». При l=5 ЛП принимает вид: $\boldsymbol{BC}_8 = \{\bigcup_{bo=1}^{n_8} BC_{8,bo}\} = \{BC_{8,1}, BC_{8,2}, BC_{8,3}, BC_{8,4}, BC_{8,5}\} = \boldsymbol{L} = \{\bigcup_{bo=1}^{5} \underset{\sim}{L}_{bo}\} = \{\underset{\sim}{L}_1, \underset{\sim}{L}_2, \underset{\sim}{L}_3, \underset{\sim}{L}_4, \underset{\sim}{L}_5\} =$ {$\underset{\sim}{H}$, $\underset{\sim}{HC}$, $\underset{\sim}{C}$, $\underset{\sim}{BC}$, $\underset{\sim}{B}$}, а лингвистическими эквивалентами используемых НЧ будут соответственно значения термов «Низкие» (Н), «Ниже среднего» (НС), «Средние» (С), «Выше среднего» (ВС) и «Высокие» (В). Здесь $BC_{8,1} = \underset{\sim}{L}_1$, $BC_{8,2} = \underset{\sim}{L}_2$, $BC_{8,3} = \underset{\sim}{L}_3$, $BC_{8,4} = \underset{\sim}{L}_4$, $BC_{8,5} = \underset{\sim}{L}_5$ – элементы базового терм-множества $\boldsymbol{L}$, отображающие расходы в виде нечетких значений. На практике встречается и интегрированное представление $\boldsymbol{L}$, например: 1) *Negligible* (менее \$100); 2) *Minor* (менее \$1000); 3) *Moderate* (менее \$10 000); 4) *Serious* (Существенное негативное влияние на бизнес); 5) *Critical* (Катастрофическое воздействие, возможно прекращение деятельности предприятия) [6, 7];

– элемент $\boldsymbol{M}$ – «**Мера риска**» ($\boldsymbol{BC}_9 = \boldsymbol{M}$), который можно представить подмножеством $\boldsymbol{BC}_9 = \{\bigcup_{bo=1}^{n_9} BC_{9,bo}\} = \boldsymbol{M} = \{\bigcup_{bo=1}^{me} M_{bo}\}$, ($\boldsymbol{BC}_9 \subseteq \boldsymbol{BC}$, $bo = \overline{1, me}$), где $n_9 = me$ – количество возможных идентификаторов меры риска. Например, при me =3 подмножество $\boldsymbol{BC}_9$ может иметь вид: $\boldsymbol{BC}_9 = \{\bigcup_{bo=1}^{n_9} BC_{9,bo}\} = \{BC_{9,1}, BC_{9,2}, BC_{9,3}\} = \boldsymbol{M} = \{\bigcup_{bo=1}^{3} M_{bo}\} = \{M_1, M_2, M_3\} =$ {«Количественная (например, характеризуемая численно)», «Качественная (например, характеризуемая лингвистически)», «Интегрированная (например, характеризуемая численно и лингвистически)»}, где $BC_{9,1} = M_1$, $BC_{9,2} = M_2$, $BC_{9,3} = M_3$ – элементы подмножества $\boldsymbol{M}$, отображающие в виде лингвистических значений соответствующую меру риска;

– элемент $\boldsymbol{P}$ – «**Вероятность**» ($\boldsymbol{BC}_{10} = \boldsymbol{P}$), который может отображаться статистическими данными. При возникновении сложности с получением статистических данных или для простоты интерпретации величин, эксперты часто используют логико-лингвистический подход. С его помощью осуществляется отображение соответствующей характеристики посредством ЛП [4-7] «Вероятность». Она определяется базовым терм-множеством, например, $\boldsymbol{BC}_{10} = \{\bigcup_{bo=1}^{n_{10}} BC_{10,bo}\} = \boldsymbol{P} = \{\bigcup_{bo=1}^{p} \underset{\sim}{P}_{bo}\}$, ($\boldsymbol{BC}_{10} \subseteq \boldsymbol{BC}$, $bo = \overline{1, p}$), где $n_{10} = p$ – количество термов ЛП «Вероятность», для членов которого справедливо

отношение порядка $\underset{\sim}{P}_1 < \underset{\sim}{P}_2 < ... < \underset{\sim}{P}_p$. Например, при p=3 подмножество $\boldsymbol{BC}_{10}$ может представляться как: $\boldsymbol{BC}_{10} = \{\bigcup_{bo=1}^{n_{10}} BC_{10,bo}\} = \{BC_{10,1}, \ BC_{10,2}, \ BC_{10,3}\} = \ \boldsymbol{P} = \{\bigcup_{bo=1}^{3} \underset{\sim}{P}_{bo}\} = \{\underset{\sim}{P}_1, \underset{\sim}{P}_2, \underset{\sim}{P}_3\} = \{\underset{\sim}{H}, \underset{\sim}{C}, \underset{\sim}{B}\}$ и отображаться НЧ $\underset{\sim}{H}$, $\underset{\sim}{C}$ и $\underset{\sim}{B}$, имеющими лингвистический эквивалент «низкая» (Н), «средняя» (С) и «высокая» (В) соответственно. Здесь $BC_{10,1} = \underset{\sim}{P}_1$, $BC_{10,2} = \underset{\sim}{P}_2$ и $BC_{10,3} = \underset{\sim}{P}_3$ – элементы базового терм-множества $\boldsymbol{P}$ отображающие значения вероятности в лингвистической форме. Как правило, для указанных НЧ на основе известных методов [4-7] формируются необходимые функции принадлежности (ФП). Также, кроме указанных, могут быть введены и другие значения первичных термов, например, «очень низкая» (ОН), «выше среднего» (ВС), «ниже среднего» (НС) и др. Очевидно, что в этом случае характеристика $\boldsymbol{P}$ отображается набором лингвистических значений, но как частный случай, она может принимать четкое или интервальное значение. В этом случае для ее отображения будем использовать не полужирный шрифт, например, *P*;

– элемент $\boldsymbol{SC}$ – «**Ситуация выбора**» ($\boldsymbol{BC}_{11} = \boldsymbol{SC}$), представляемый ЛП «СИТУАЦИЯ ВЫБОРА» с базовым терм-множеством $\boldsymbol{BC}_{11} = \{\bigcup_{bo=1}^{n_{11}} BC_{11,bo}\} = \ \boldsymbol{SC} = \{\bigcup_{bo=1}^{sc} \underset{\sim}{SC}_{bo}\}$, $(\boldsymbol{BC}_{11} \subseteq \boldsymbol{BC}, \ bo = \overline{1, sc})$, где $n_{11} = sc$ – количество термов указанной ЛП, для которых справедливо отношения порядка $\underset{\sim}{SC}_1 < \underset{\sim}{SC}_2 < ... < \underset{\sim}{SC}_{sc}$. С помощью $\boldsymbol{SC}$ можно интерпретировать выбор посредством *sc* вариантов. Например, при sc=2 для указанной ЛП могут быть сформированы подмножества $\boldsymbol{BC}_{11} = \{\bigcup_{bo=1}^{n_{11}} BC_{11,bo}\} = \ \{BC_{11,1}, BC_{11,2}\} = \ \boldsymbol{SC} = \{\bigcup_{bo=1}^{2} \underset{\sim}{SC}_{bo}\} = \ \{\underset{\sim}{SC}_1, \underset{\sim}{SC}_2\} =$ {«Менее привлекательная (МП)», «Более привлекательная (БП)»} или $\boldsymbol{SC} = \{\bigcup_{bo=1}^{2} \underset{\sim}{SC}_{bo}\} =$ {«Менее надежная (МН)», «Более надежная (БН)»}, которые соответственно отображаются НЧ $\underset{\sim}{\text{МП}}, \underset{\sim}{\text{БП}}$ или $\underset{\sim}{\text{МН}}, \underset{\sim}{\text{БН}}$, где $BC_{11,1} = \underset{\sim}{SC}_1$, $BC_{11,2} = \underset{\sim}{SC}_2$ – элементы базового терм-множества $\boldsymbol{SC}$, отображающие ситуацию выбора в виде нечетких значений;

– элемент $\boldsymbol{V}$ – «**Уязвимость**» ($\boldsymbol{BC}_{12} = \boldsymbol{V}$), который можно отобразить подмножеством идентификаторов уязвимостей $\boldsymbol{BC}_{12} = \{\bigcup_{bo=1}^{n_{12}} BC_{12,bo}\} = \boldsymbol{V} = \{\bigcup_{bo=1}^{n} V_{bo}\}$, $(\boldsymbol{BC}_{12} \subseteq \boldsymbol{BC}, bo = \overline{1,n})$, где $n_{12} = n$ – количество возможных уязвимостей (и соответственно их идентификаторов) РИС. Например, при n=3 подмножество $\boldsymbol{BC}_{12} = \{\bigcup_{bo=1}^{3} BC_{12,bo}\} = \{BC_{12,1}, BC_{12,2}, BC_{12,3}\} = \boldsymbol{V}$ может иметь следующий вид $\boldsymbol{V} = \{\bigcup_{bo=1}^{3} V_{bo}\} = \{V_1, V_2, V_3\} =$ {«Нулевого дня», «Переполнение буфера», «SQL-инъекция»}, где $BC_{12,1} = V_1$, $BC_{12,2} = V_2$, $BC_{12,3} = V_3$ – элементы подмножества идентификаторов $\boldsymbol{V}$, отображающих идентифицированные уязвимости РИС, связанные соответственно с угрозами нулевого дня, переполнением буфера и реализацией SQL-инъекции;

– элемент VA – «**Оценка CVSS**» ($\boldsymbol{BC}_{13} = \boldsymbol{VA}$), который может отображаться подмножеством $\boldsymbol{BC}_{13} = \{\bigcup_{bo=1}^{n_{13}} BC_{13,bo}\} = \ \boldsymbol{VA} = \{\bigcup_{bo=1}^{va} VA_{bo}\}$, $(\boldsymbol{BC}_{13} \subseteq \boldsymbol{BC}, \ bo = \overline{1, va})$, где $n_{13} = va$ – количество идентификаторов версии CVSS, например, при va=2 $\boldsymbol{BC}_{13} = \{\bigcup_{bo=1}^{n_{13}} BC_{13,bo}\} = \{BC_{13,1}, BC_{13,2}\} = \boldsymbol{VA} = \{\bigcup_{bo=1}^{2} VA_{bo}\} = \{VA_1, VA_2\} =$ {«CVSS v02», «CVSS v03»}, ($BC_{13,1} = VA_1$, $BC_{13,2} = VA_2$ – идентификаторы версии CVSS). Этот элемент отражает наличие в системе информации об используемой версии CVSS оценки.

На основе множества $\boldsymbol{BC}$, а также с учетом анализа проведенного в [6-8, 13], предлагается формировать два базовых подмножества:

– первое назовем идентифицирующее – $\{\bigcup_{i=1}^{ind}\boldsymbol{ABC}_i\} = \{\bigcup_{i=1}^{ind}\{\bigcup_{bo=1}^{abc_i} ABC_{i,bo}\}\} =$

$\{\bigcup_{i=1}^{ind}\{ABC_{i,1}, ABC_{i,2}, ..., ABC_{i,abc_i}\}\} =$

$\{\{ABC_{1,1}, ABC_{1,2}, ..., ABC_{1,abc_1}\},$

$\{ABC_{2,1}, ABC_{2,2}, ..., ABC_{2,abc_2}\}, ...,$

$\{ABC_{ind,1}, ABC_{ind,2}, ..., ABC_{ind,abc_{ind}}\}\}$

($\boldsymbol{ABC}_i \subseteq \boldsymbol{BC}$, $i = \overline{1, ind}$, $bo = \overline{1, abc_i}$);

– второе назовем оценочное – $\{\bigcup_{i=1}^{ass}\boldsymbol{SBC}_i\} =$

$\{\bigcup_{i=1}^{ass}\{\bigcup_{bo=1}^{sbc_i} SBC_{i,bo}\}\} =$

$\{\bigcup_{i=1}^{ass}\{SBC_{i,1}, SBC_{i,2}, ..., SBC_{i,sbc_i}\}\} =$

$\{\{SBC_{1,1}, SBC_{1,2}, ..., SBC_{1,sbc_1}\},$

$\{SBC_{2,1}, SBC_{2,2}, ..., SBC_{2,sbc_2}\}, ...,$

$\{SBC_{ass,1}, SBC_{ass,2}, ..., SBC_{ass,sbc_{ass}}\}\}$ ($\boldsymbol{SBC}_i \subseteq \boldsymbol{BC}$, $i = \overline{1, ass}$, $bo = \overline{1, sbc_i}$), где ind и ass – соответственно количество идентифицирующих и оценочных характеристик риска ИБ, используемых для его анализа и оценивания.

Так, например, при bc=13 и ind =9 можно составить следующее идентифицирующее подмножество характеристик риска: $\{\bigcup_{i=1}^{9}\boldsymbol{ABC}_i\} = \{\boldsymbol{ABC}_1, \boldsymbol{ABC}_2, \boldsymbol{ABC}_3, \boldsymbol{ABC}_4, \boldsymbol{ABC}_5, \boldsymbol{ABC}_6, \boldsymbol{ABC}_7, \boldsymbol{ABC}_8, \boldsymbol{ABC}_9\} = \{\boldsymbol{AES}, \boldsymbol{CA}, \boldsymbol{CS}, \boldsymbol{DT}, \boldsymbol{E}, \boldsymbol{M}, \boldsymbol{SC}, \boldsymbol{V}, \boldsymbol{VA}\}$, где $\boldsymbol{ABC}_1 = \boldsymbol{AES}$, $\boldsymbol{ABC}_2 = \boldsymbol{CA}$, $\boldsymbol{ABC}_3 = \boldsymbol{CS}$, $\boldsymbol{ABC}_4 = \boldsymbol{DT}$, $\boldsymbol{ABC}_5 = \boldsymbol{E}$, $\boldsymbol{ABC}_6 = \boldsymbol{M}$, $\boldsymbol{ABC}_7 = \boldsymbol{SC}$, $\boldsymbol{ABC}_8 = \boldsymbol{V}$, $\boldsymbol{ABC}_9 = \boldsymbol{VA}$, а при ass =4 – оценочное подмножество характеристик риска: $\{\bigcup_{i=1}^{4}\boldsymbol{SBC}_i\} = \{\boldsymbol{SBC}_1, \boldsymbol{SBC}_2, \boldsymbol{SBC}_3, \boldsymbol{SBC}_4\} = \{\boldsymbol{D}, \boldsymbol{F}, \boldsymbol{L}, \boldsymbol{P}\}$, где $\boldsymbol{SBC}_1 = \boldsymbol{D}$, $\boldsymbol{SBC}_2 = \boldsymbol{F}$, $\boldsymbol{SBC}_3 = \boldsymbol{L}$, $\boldsymbol{SBC}_4 = \boldsymbol{P}$.

Далее, для эффективной организации процесса анализа существующих средств оценивания и их разработки осуществляется интеграция членов представленных подмножеств характеристик риска посредством их отображения в двух фиксированных кортежах (см. рис. 1). Первый кортеж – аналитический (АК), используемый для анализа средств оценивания с целью последующего их выбора. Второй кортеж – синтетический (СК), используемый для помощи разработчикам, синтезирующих такие средства оценивания. Как видно из структурно-аналитического представления БИМ (АСМ) (см. рис. 1) основу указанных кортежей составляет множество $\boldsymbol{BC}$ и подмножества $\boldsymbol{ABC}_i$, $\boldsymbol{SBC}_i$. Рассмотрим конкретный пример их использования в БИМ (АСМ).

Пусть для исследования средств анализа и оценивания рисков необходимо в качестве соответствующих сравнительных характеристик воспользоваться: возможностью адаптации нечеткой шкалы оценивания, т.е. возможности системы трансформировать эталоны (см. элемент $\boldsymbol{AES}$); калькулятором для оценивания риска или оценок CVSS (см. элемент $\boldsymbol{CA}$); информацией об отклонении от поставленной цели, например, в бизнесе (см. элемент $\boldsymbol{DT}$); возможностью оценивания рисков относительно нарушений базовых характеристик ИБ РИС (см. элемент $\boldsymbol{E}$); возможностью выбора (см. элемент $\boldsymbol{SC}$); информацией об уязвимостях РИС (см. элемент $\boldsymbol{V}$); возможностью использования оценок CVSS (см. элемент $\boldsymbol{VA}$), возможностью определения среды оценивания, в которой работает исследуемое средство (см. элемент $\boldsymbol{CS}$); параметрами для оценивания, например, идентифицированных уязвимостей РИС (см. элементы $\boldsymbol{P}$, $\boldsymbol{D}$, $\boldsymbol{F}$ и $\boldsymbol{L}$); форматом представления данных в анализируемом средстве (см. элемент $\boldsymbol{M}$), то можно сформировать АК, который имеет следующий вид (см. рис. 1): $\langle \boldsymbol{ABCM}_1, \boldsymbol{ABCM}_2, ..., \boldsymbol{ABCM}_{an} \rangle$, где $\boldsymbol{ABCM}_i$ – компонент АК ($i = \overline{1, an}$), а an – количество членов АК.

Для подмножеств $\boldsymbol{ABC}_i$ и $\boldsymbol{SBC}_i$ в выше рассмотренном примере, АК может иметь следующий вид (an=13):

$\langle \boldsymbol{ABCM}_1, \boldsymbol{ABCM}_2, \boldsymbol{ABCM}_3, \boldsymbol{ABCM}_4, \boldsymbol{ABCM}_5, \boldsymbol{ABCM}_6, \boldsymbol{ABCM}_7, \boldsymbol{ABCM}_8, \boldsymbol{ABCM}_9, \boldsymbol{ABCM}_{10}, \boldsymbol{ABCM}_{11}, \boldsymbol{ABCM}_{12}, \boldsymbol{ABCM}_{13} \rangle =$

$\langle \boldsymbol{AES}, \boldsymbol{CA}, \boldsymbol{CS}, \boldsymbol{D}, \boldsymbol{DT}, \boldsymbol{E}, \boldsymbol{F}, \boldsymbol{L}, \boldsymbol{M}, \boldsymbol{P}, \boldsymbol{SC}, \boldsymbol{V}, \boldsymbol{VA} \rangle$,

где $\boldsymbol{ABCM}_1 = \boldsymbol{ABC}_1 = \boldsymbol{AES}$, $\boldsymbol{ABCM}_2 = \boldsymbol{ABC}_2 =$

CA, $ABCM_3 = ABC_3 = CS$, $ABCM_5 = ABC_4 = DT$, $ABCM_6 = ABC_5 = E$, $ABCM_9 = ABC_6 = M$, $ABCM_{11} = ABC_7 = SC$, $ABCM_{12} = ABC_8 = V$, $ABCM_{13} = ABC_9 = VA$ определяются с помощью подмножества ABC_i, а $ABCM_4 = SBC_1 = D$, $ABCM_7 = SBC_2 = F$, $ABCM_8 = SBC_3 = L$, $ABCM_{10} = SBC_4 = P$ – с помощью подмножества SBC_i.

Также, например, если при синтезе соответствующих средств оценивания разработчикам необходимо в качестве характеристик воспользоваться: возможностью адаптации нечеткой шкалы оценивания (см. элемент AES); встроенными калькуляторами для оценивания риска и оценок CVSS (см. элемент CA); информацией об уязвимостях РИС (см. элемент V); возможностью оценивания рисков относительно нарушений базовых характеристик ИБ РИС (см. элемент E); параметрами для оценивания идентифицированных уязвимостей РИС (см. элементы D, F, L, P), то в этом случае можно сформировать СК, который имеет вид: $\langle SBCM_1, SBCM_2, ..., SBCM_{dev} \rangle$, где $SBCM_i$ – компонент СК ($i = \overline{1, dev}$), dev – количество членов СК. Для подмножеств ABC_i и SBC_i в выше рассмотренном примере, СК может иметь следующий вид (dev=8): $\langle SBCM_1, SBCM_2, SBCM_3, SBCM_4, SBCM_5, SBCM_6, SBCM_7, SBCM_8 \rangle = \langle AES, CA, D, E, F, L, P, V \rangle$, где $SBCM_1 = ABC_1$, $SBCM_2 = ABC_2$, $SBCM_4 = ABC_3$, $SBCM_8 = ABC_8$ определяются с помощью подмножества ABC_i, а $SBCM_3 = SBC_1$, $SBCM_5 = SBC_2$, $SBCM_6 = SBC_3$, $SBCM_7 = SBC_4$ – с помощью подмножества SBC_i.

Таким образом, в работе усовершенствована базовая интегрированная кортежная модель, которая за счет разделения определенного множества всех базовых характеристик риска на подмножества идентифицирующих и оценочных компонент, отображаемых посредством двух фиксированных кортежей – аналитическим (который используется для исследования широкого спектра существующих средств анализа и оценивания риска с позиций формирования необходимых для их функционирования исходных данных) и синтетическим (который используется для помощи разработчикам, синтезирующих соответствующие средства оценивания), позволит упростить принятие решения о выборе необходимого средства оценивания и выбор необходимого набора параметров при создании систем оценивания рисков.

ЛИТЕРАТУРА

[1]. Ахметов Б.С. Метод n-кратного понижения порядка лингвистических переменных на основе частного расширения базы / Б.С. Ахметов, С.В. Казмирчук, А.Ю. Гололобов, С.А. Гнатюк, Н.А. Сейлова // Безпека інформації. – 2014. – Т.20. –№3. – С. 306-311.

[2]. Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С.О. Гнатюк // Безпека інформації – 2013. – №2. – С. 118-129.

[3]. Казмирчук С.В. Метод трансформирования термов лингвистических переменных в задачах анализа и оценивания рисков информационной безопасности / С.В. Казмирчук // Захист інформації. – 2013. – Т.15. – №3, липень-вересень. – С. 268-276.

[4]. Корченко А.А. Метод определения идентифицирующих термов для систем обнаружения вторжений / А.А. Корченко // Безпека інформації – 2014. – №3. – С. 217-223.

[5]. Корченко А.А. Метод фаззификации параметров на лингвистических эталонах для систем выявления кибератак / А.А. Корченко // Безпека інформації – 2014. – №1. – С. 21-28.

[6]. Корченко А.Г. Анализ и оценивание рисков информационной безопасности. Монография. / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук – К. : ООО «Лазурит-Полиграф», 2013. – 275 с.

[7]. Корченко А.Г. Интегрированное представление параметров риска / А.Г. Корченко, Е.В. Иванченко, С.В. Казмирчук // Защита информации – 2011. – №1 (50). – С. 96-101.

[8]. Корченко А.Г. Качественно-количественный метод оценивания рисков информационной безопасности / А.Г. Корченко, С.В. Казмирчук // Захист інформації. – 2016. –№2. – С. 157-170.

[9]. Корченко А.Г. Метод n-кратного инкрементирования порядка лингвистических переменных на основе частного расширения базы / А.Г. Корченко, Б.С. Ахметов, С.В. Казмирчук, М.Н. Жекамбаева // Захист інформації. – 2015. –№3. – С. 231-239.

[10]. Корченко А.Г. Метод n-кратного инкрементирования числа термов лингвистических переменных в задачах анализа и оценивания рисков / А.Г. Корченко, С.В. Казмирчук, Б.С. Ахметов, М.Н. Жекамбаева // Безпека інформації. – 2015. – Т.21. –№2. – С. 191-200.

[11]. Корченко А.Г. Метод n-кратного понижения числа термов лингвистических переменных в задачах анализа и оценивания рисков / А.Г. Корченко, Б.С. Ахметов, С.В. Казмирчук, А.Ю. Гололобов, Н.А. Сейлова // Захист інформації. – 2014. – Т.16. – №4, жовтень-грудень. – С. 284-291.

[12]. Корченко А.Г. Метод инкрементирования порядка лингвистических переменных для систем анализа и оценивания рисков / А.Г. Корченко, С.В. Казмирчук, Ю.Б. Коваленко, А.Ю. Гололобов // Захист інформації. – 2015. – Т.17. – №2, квітень-червень. – С. 100-108.

[13]. Корченко А.Г. Метод оценивания рисков информационной безопасности на основе открытых баз данных уязвимостей / А.Г. Корченко, С.В. Казмирчук // Безпека інформації. – 2016. –№2. – С. 216-226.

[14]. Корченко А.Г. Метод преобразования эталонов параметров для систем анализа и оценивания рисков информационной безопасности / А.Г. Корченко, С.В. Казмирчук, А.Ю. Гололобов // Захист інформації. – 2013. – Т.15. – №4, жовтень-грудень. – С. 359-366.

[15]. Корченко А.Г. Метод реализации функции трансформирования эталонов в задачах анализа и оценивания рисков / А.Г. Корченко, Б.С. Ахметов, С.В. Казмирчук, А.Ю. Гололобов // Безпека інформації. – 2015. – Т.21. – №1. – С. 104-112.

[16]. Шаховал О.А. Рекомендації щодо розробки стратегії забезпечення кібербезпеки України / О.А. Шаховал, І.Л. Лозова, С.О. Гнатюк // Защита информации – 2016. – №1 – С. 57-65.

REFERENCES

[1]. Akhmetov B., Kazmirchuk S., Gololobov A., Gnatyuk S., Seylova N. The n-fold decrease method of linguistics variables, based on the private database extension, Bezpeka informatsiyi, 2014, VOL.20 №3, pp. 306-311.

[2]. Gnatyuk S.O. Cyberterrorism: development history, current trends & countermeasures, Bezpeka informatsiyi, 2013, VOL.19 №2, pp. 118-129.

[3]. Kazmirchuk S. The method of terms transformation of linguistic variables in decision-making analysis and information security risk assessment, Zahist ìnformacìï, 2013, VOL. 15 №3, pp. 268-276.

[4]. Korchenko A. The detection method of identification terms for intrusion detection system, Bezpeka informatsiyi, 2014, VOL.20 №3, pp. 217-223.

[5]. Korchenko A. Method of parameter fuzzification based on linguistic standards for cyber attacks detection, Bezpeka informatsiyi, 2014, VOL.20 №1, pp. 21-28.

[6]. Korchenko A.G., Kazmirchuk S.V., Arkhipov A.E. The analysis and assessment risks information security. Monograph, 2013, 275 p.

[7]. Korchenko A., Ivanchenko E., Kazmirchuk S. An integrated view of risk parameters, Zahist ìnformacìï, 2011, №1, pp. 96-101.

[8]. Korchenko A., Kazmirchuk S. The qualitative and quantitative method of information security risk assessment, Zahist ìnformacìï, 2016, №2, pp. 157-170.

[9]. Korchenko A., Akhmetov B., Kazmirchuk S., Zhekambaeva M. n-fold incrementation of linguistic variables order method, based on particular base expansion, Zahist ìnformacìï, 2015, №3, pp. 231-239.

[10]. Korchenko A., Akhmetov B., Kazmirchuk S., Zhakambayeva M. Method of n-fold incrementation the number of terms the linguistic variables in the tasks of analysis and risk assessment, Bezpeka informatsiyi, 2015, VOL.21 №2, pp. 191-200.

[11]. Korchenko A., Akhmetov B., Kazmirchuk S., Gololobov A., Seylova N. The n-fold decrease method of terms number of linguistic variables in risk assessment and task analysis, Zahist ìnformacìï, 2014, №4, pp. 284-291.

[12]. Korchenko A., Kazmirchuk S., Kovalenko J., Gololobov A. Method of increment order of linguistic variables for risk analysis and assessment systems, Zahist ìnformacìï, 2015, №2, pp. 100-108.

[13]. Korchenko O., Kazmirchuk S. The risk assessment method of information security based on open databases vulnerabilities, Bezpeka informatsiyi, 2016, VOL.22 №2, pp. 216-226.

[14]. Korchenko O., Kazmirchuk S., Gololobov A. The conversion method of reference parameters for

systems analysis and information security risk assessment, Zahist ìnformacìï, 2013, №4, pp. 359-366.
[15]. Korchenko O., Akhmetov B., Kazmirchuk S., Gololobov A. Method of function realization for transformation etalons in risk analysis and assessment, Bezpeka informatsiyi, 2015, VOL.21 №1, pp. 104-112.
[16]. Shahoval O., Lozova I., Gnatyuk S. Recommendations for cybersecurity strategy of ukraine development, Zahist ìnformacìï, 2016, №1, pp. 57-65.

БІСТАБІЛЬНА ІНТЕГРОВАНА КОРТЕЖНА МОДЕЛЬ ХАРАКТЕРИСТИК РИЗИКУ

Часто перед фахівцями відповідних підприємств, для підвищення ефективності вирішення завдань захисту інформації, виникає питання про вибір існуючих або розробку нових засобів оцінювання ризиків безпеки ресурсів інформаційних систем. Перш ніж здійснювати такий вибір або розробку необхідно мати достатньо повне відображення характеристик ризику в аспекті інформаційної безпеки. У зв'язку з цим, в роботі визначені множини базових характеристик ризику для галузі інформаційної безпеки. На підставі цього пропонується відображати задані ідентифікуючи і оціночні характеристики у вигляді бістабільної (біфіксованої) інтегрованої кортежної моделі. На практиці таку модель пропонується використовувати у вигляді відображення на два частних кортежі – аналітичний і синтетичний, які застосовуються відповідно для реалізації вибору існуючих засобів і для допомоги розробникам при створенні нових систем оцінювання ризиків.

Ключові слова: аналіз ризику, оцінювання ризику, базові характеристики ризику, бістабільних інтегрована кортежних модель, приватна відображення кортежу, ризик інформаційної безпеки, лінгвістична змінна.

BISTABLE AND INTEGRATED BASED TUPLE MODEL OF RISK CHARACTERISTICS

Often experts of corresponding companies in order to increase the efficiency of information security decision making, put the question on the choice of existing or development of new means of security risks assessment of information systems resources. For the effective organization of appropriate process of a choice or development it is necessary to have a complete display of risk characteristics. In this regard, the most of the basic characteristics of risk for the information security sphere are defined in the work. According to this, it is proposed to display the characteristics of identification and assessment as a bistable integrated model of a tuple. In practice such model is offered to be used as a display on two particular tuples – analytical and synthetic, applied according to the choice implementation of existing means and to assist developers at creation of new risk assessment systems.

Keywords: Risk analysis, risk assessment, the basic characteristics of risk, bistable and integrated based tuple model, the partial display of the tuple, information security risk, linguistic variable.

Корченко Александр Григорьевич, доктор технических наук, профессор, лауреат Государственной премии Украины в области науки и техники, заведующий кафедрой безопасности информационных технологий Национального авиационного университета, старший научный сотрудник Национальной академии СБ Украины.
E-mail: icaocentre@nau.edu.ua
Корченко Олександр Григорович, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету, старший науковий співробітник Національної академії СБ України.
Korchenko Oleksandr, Dr Eng (Information security), professor, laureate of the State Prize of Ukraine in Science and Technology, Head of IT-Security Academic Department, National Aviation University, Senior Researcher of the National Academy of SS of Ukraine.

Казмирчук Светлана Владимировна, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: sv.kazmirchuk@gmail.com
Казмірчук Світлана Володимирівна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Kazmirchuk Svitlana, PhD in Eng., Associate Professor of IT-Security Academic Department, National Aviation University.

Дрейс Юрий Александрович, кандидат технических наук, доцент, заведующий кафедрой дистанционного обучения Национального авиационного университета.
E-mail: y.dreis@nau.edu.ua
Дрейс Юрій Олександрович, кандидат технічних наук, доцент, завідувач кафедри дистанційного нав- чання Національного авіаційного університету.
Dreis Yurii, PhD in Eng., Associate Professor, Head of Distance e-Learning Academic Department, National Aviation University (Kyiv, Ukraine).
Гололобов Андрей Юрьевич, аспирант кафедры безопасности информационных технологий Нацио- нального авиационного университета.
E-mail: burn2dust@gmail.com.
Гололобов Андрій Юрійович, аспірант кафедри безпеки інформаційних технологій Національного авіаційного університету.
Gololobov Andrew, postgraduate student of IT-Security Academic Department, National Aviation University.

DOI: 10.18372/2410-7840.18.11085
УДК 004.421.5

ГЕНЕРУВАННЯ ВИПАДКОВИХ ЧИСЕЛ ШТАТНИМИ ЗАСОБАМИ ХОСТІВ МЕРЕЖІ ІНТЕРНЕТ

Володимир Чуприн, Володимир Вишняков, Михайло Пригара

У системах опитування або голосування через мережу Інтернет з метою забезпечення умов для вільного висловлювання думки опитуваних необхідно збереження таємниці голосів. Для цього використовують криптографічний захист інформації, який потребує генерування випадкових чисел. Вкрай бажано, щоб ці числа були дійсно, а не псевдовипадковими. Генератори дійсно випадкових чисел (ГВЧ), що використовують у складі підсистем захисту серверних частин систем голосування, мають відповідати ряду критеріїв, зокрема вимогам НД ТЗІ, оскільки домени безпеки серверного обладнання систем голосування в багатьох випадках мають бути сертифікованими відповідним уповноваженим органом. У той же час вимога щодо обов'язкової сертифікації за критеріями ТЗІ клієнтського обладнання систем голосування, як правило, не висувається, оскільки бажано, щоб виборець мав можливість здійснювати акти волевиявлення за допомогою виключно штатних засобів будь-якого хоста. Саме можливість голосування з будь-якого хоста без будь-яких спеціальних зусиль та засобів є найбільш привабливою властивістю систем дистанційного голосування. У даній роботі пропонується механізм отримання дійсно (не псевдо) випадкових чисел на будь-яких клієнтських вузлах мережі Інтернет без додаткових програмних засобів або фізичних пристроїв. Для цього пропонується скористатися випадковим характером нестабільності частот двох кварцових резонаторів (таймерного та тактового), що входять до складу будь-якого комп'ютера, та випадковим характером потоку запитів, що надходять на порти цього комп'ютера із мережі Інтернет. Проведено експериментальні дослідження запропонованого механізму. Теоретично доведена неможливість передбачати отримані числа в заданих умовах використання, що свідчить про недоцільність будь-яких спроб їх розкриття за допомогою крипто аналізу.

Ключові слова: *Інтернет-голосування, клієнтський хост, технічний захист інформації, генерування випадкових чисел, нестабільність кварцових резонаторів, потік запитів із Інтернет, самоподібний процес.*

ВСТУП. Захист інформації в системах опитування або голосування з використанням мережі Інтернет повинен забезпечувати умови для вільного висловлювання думки опитуваних. Зрозуміло, що тільки у випадку впевненості у неможливості розкриття результату волевиявлення людина може висловлюватись вільно. Загально відомо, що довіру виборців заслуговують лише ті системи, які є прозорими для контролю з боку виборчої спільноти. На прикладі системи опитування «Викладач очима студентів», з якою можна ознайомитись на сайті http://fit.univ.kiev.ua/archives/3246, легко зрозуміти, що у разі розкриття викладачами інформації про те, як проголосували конкретні студенти, з'являється можливість упередженого ставлення до цих студентів на іспитах. Тому через відсутність досконалого захисту інформації про голоси студентів неможливо забезпечити об'єктивність результатів опитування, що дискредитує саму ідею подібного заходу. На рівні державних виборів таємниця голосів є обов'язковою, що вказано, зокрема, у Міжнародному Пакті від 16 грудня 1966 р. «Про громадянські та політичні права». Труд-