© Korchenko A., Kazmirchuk S. The risk assessment method of information security based on open databases vulnerabilities // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 2, p. 214-224.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATION SECURITY MANAGEMENT

МЕТОД ОЦЕНИВАНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ОТКРЫТЫХ БАЗ ДАННЫХ УЯЗВИМОСТЕЙ

Александр Корченко, Светлана Казмирчук

Национальный авиационный университет, Украина

КОРЧЕНКО Александр Григорьевич, д.т.н.

Год и место рождения: 1961 год, г. Киев, Украина.
Образование: Киевский институт инженеров гражданской авиации (с 2000 года - Национальный авиационный университет), 1983 год.
Должность: заведующий кафедрой безопасности информационных технологий, НАУ, Визит-профессор, Университет в Бельско-Бялой (г. Бельско-Бяла, Польша) .
Научные интересы: информационная и авиационная безопасность.
Публикации: более 300 научных публикаций, среди которых монографии, словари, учебники, учебные пособия, научные статьи и патенты на изобретения.
E-mail: agkorchenko@gmail.com

КАЗМИРЧУК Светлана Владимировна, к.т.н.

Год и место рождения: 1985 год, г. Алматы, Республика Казахстан.
Образование: Национальный авиационный университет, 2006 год.
Должность: доцент кафедры безопасности информационных технологий с 2012 года.
Научные интересы: информационная безопасность, системы менеджмента информационной безопасности, защита программного обеспечения, комплексные системы защиты информации, управления информационными рисками.
Публикации: более 60 научных публикаций, среди которых монографии, учебные пособия, учебно-методические комплексы дисциплин, научные статьи и материалы и тезисы докладов на конференциях.
E-mail: sv.kazmirchuk@gmail.com

Аннотация. *В основу построения различных систем защиты информации положен процесс оценивания рисков. Для его реализации применяются известные методы анализа и оценивания рисков, основанные на экспертных оценках. Часто в процессе оценивания приходится сталкиваться с ситуациями, при которых возникают сложности с привлечением экспертов или они не всегда четко могут оценить ту или иную уязвимость ресурсов информационных систем. Также при практическом использовании таких систем возникает необходимость оперативного оценивания и мониторинга (в реальном времени) рисков без привлечения экспертов. В связи с этим целесообразно использовать соответствующие базы данных уязвимостей. Существующие подходы пока не позволяют эффективно решать поставленные задачи. Для этого предлагается метод оценивания рисков на основе открытых баз данных уязвимостей. Он, в отличие от известных методов, путем использования оценок, которые предоставляются в существующих базах данных, позволяет автоматизировать процесс оценивания рисков без привлечения экспертов соответствующей предметной области.*

Ключевые слова: *риск, оценивание рисков, система оценивания рисков, параметры риска, нечеткая переменная, нечеткие числа, преобразования эталонов нечетких чисел, метод оценивания рисков, открытые база данных уязвимостей.*

Задача оценивания рисков (ОР) информационной безопасности (ИБ), согласно требованиям международных или государственных стандартов [11, 13], является основополагающей при создании соответствующих систем защиты информации (ЗИ). Решения таково рода задачи дает возможность определить более эффективные меры ЗИ. Для ее реализации применяются методы ОР [2, 5, 6], которые основываются на экспертных оценках. Часто при ОР не всегда имеется возможность привлечения экспер-

тов соответствующей предметной области. На практике, например, могут возникать ситуации, при которых необходимо реализовывать оперативное оценивание и мониторинг (в реальном времени) рисков без привлечения указанных экспертов, а доступные методы и средства ОР [2, 5, 6] не дают такой возможности.

Для этого предлагается использовать соответствующие открытые базы данных (БД) уязвимостей ресурсов информационных систем (РИС), в которых представлены их количественные оценки, например, такие как национальная база данных уязвимостей (США) (National Vulnerability Database (NVD)) [15]; банк данных угроз безопасности информации (Российская Федерация) [1]; открытая база данных уязвимостей (США) (Open Sourced Vulnerability Database OSVDB)) [16]; база данных уязвимостей IBM X-Force (США) [12], база данных записей уязвимостей US-CERT VND (США) [18], база данных уязвимостей SecurityFocus (США) [17] и т.д. Базовой составляющей таких БД являются CVSS (Common Vulnerability Scoring System) [14] – показатели, которые можно использовать в качестве альтернативы оценкам экспертов. Поэтому разработка метода ОР с использованием выше представленные БД и автоматизации процесса оценивания без участия экспертов, является актуальной задачей.

В связи с этим, цель данной работы направлена на разработку метода ОР, который позволит осуществить оценивание рисков с использованием открытых БД не привлекая экспертов соответствующей предметной области.

В основу такого метода положены исследования проведенные в [2, 5, 6]. Рассмотрим детально его работу, которая основывается на 11 шагах.

Шаг 1 (Определение полного множества идентификаторов РИС и уязвимостей) и **Шаг 2 (Определение множества идентификаторов РИС и уязвимостей для объекта оценивания)** аналогичен качественно-количественному методу ОР ИБ описанному в [6].

Шаг 3 (Определение множества параметров оценивания риска). Здесь введем множество оценок риска $\boldsymbol{LR}$ для определенного на втором шаге (см. [6]) $\boldsymbol{RISO}$, т.е. при $rs=\overline{1,ro}$ $\exists \boldsymbol{LR}=\{\bigcup_{rs=1}^{ro} LR_{rs}\}=\{LR_1,...,\ LR_{rs}\}$. Также для ОР по каждой уязвимости, отображенной идентификатором $V_{rs,uz}$ введем множества $\boldsymbol{LRV}_{rs}$ при $rs=\overline{1,ro}$ и $uz=\overline{1,n_{rs}}$, т.е. $\exists\{\bigcup_{rs=1}^{ro}\boldsymbol{LRV}_{rs}\}=\{\bigcup_{rs=1}^{ro}\{\bigcup_{uz=1}^{n_{rs}} LRV_{rs,uz}\}\}$, где $LRV_{rs,uz}$ – количественная оценка риска по каждой uz-той уязвимости rs-того РИС на объекте.

Для отображения результата ОР воспользуемся лингвистической переменной (ЛП) «СТЕПЕНЬ РИСКА» ($\boldsymbol{DR}$), представленной в виде кортежа [2-6] $<\boldsymbol{DR},\ \underset{\sim}{T}^{DR},\ \boldsymbol{X}_{DR}>$, где базовые терм-множества определяются m термами $\underset{\sim}{\boldsymbol{T}}^{DR}=\bigcup_{j=1}^{m}\underset{\sim}{T}^{DR_j}$. Для каждого из термов $\underset{\sim}{T}^{DR_1},\ldots,\underset{\sim}{T}^{DR_j},\ldots,\underset{\sim}{T}^{DR_m}$ соответственно задается свой интервал значений $[dr_1;\ dr_2[,\ \ldots,\ [dr_j;\ dr_{j+1}[,\ldots,\ [dr_m;\ dr_{m+1}]$.

Далее для обеспечения процесса оценивания берутся за основу показатели CVSS [14] из NVD [15]. Для этого определим необходимые множества параметров $\boldsymbol{EP}_i$, $(i=\overline{1,g})$, используемых для оценивания, т.е. $\boldsymbol{EP}=\{\bigcup_{i=1}^{g}\boldsymbol{EP}_i\}=\{EP_1, EP_2,...,\ EP_g\}$, где g – количество множеств таких параметров.

Отметим, что *для версии 3 оценок CVSS* [14], в которой, в отличие от версии 2.0, метрики эксплуатируемости ($\boldsymbol{AC}$, $\boldsymbol{AV}$, $\boldsymbol{PR}$, $\boldsymbol{UI}$) рассчитываются для уязвимого компонента, а метрики воздействия ($\boldsymbol{C}$, $\boldsymbol{I}$, $\boldsymbol{A}$) для атакуемого. Это дает возможность различить уязвимый и атакуемый компоненты, например, при g=3 могут быть определенны следующие множества значений – $\{\bigcup_{i=1}^{3}\boldsymbol{EP}_i\}=\{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_3\}=\{\boldsymbol{B},\ \ \boldsymbol{T},\ \ \boldsymbol{E}\}$, $(i=\overline{1,3})$, где: $\boldsymbol{B}$ – базовые (Base) оценки, представляемые в виде множества $\boldsymbol{B}=\{\bigcup_{uz=1}^{n_{rs}} B_{uz}\}$, $(uz=\overline{1,n_{rs}})$, члены которого определяются посредством группы множеств параметров $\boldsymbol{AV}_{uz}$, $\boldsymbol{AC}_{uz}$, $\boldsymbol{PR}_{uz}$, $\boldsymbol{S}_{uz}$, $\boldsymbol{UI}_{uz}$, $\boldsymbol{C}_{uz}$, $\boldsymbol{I}_{uz}$, $\boldsymbol{A}_{uz}$, $(uz=\overline{1,n_{rs}})$, где: $\boldsymbol{AV}_{uz}$ – вектор кибератаки, который представляется в виде множества $\boldsymbol{AV}_{uz}=\{\bigcup_{av=1}^{4} AV_{uz,av}\}=\{AV_{uz,1},...,AV_{uz,4}\}=\{N, A, L, P\}$, $(uz=\overline{1,n_{rs}},\ av=\overline{1,4})$ (где: N – «Сеть» = 0,85; A – «Сопряженная сеть» = 0,62; L – «Локальный доступ» = 0,55; P – «Физический доступ» = 0,2); $\boldsymbol{AC}_{uz}$ – сложность кибератаки, представляемая множеством $\boldsymbol{AC}_{uz}=\{\bigcup_{ac=1}^{2} AC_{uz,ac}\}=\{AC_{uz,1}, AC_{uz,2}\}=\{L, H\}$, $(uz=\overline{1,n_{rs}},\ ac=\overline{1,2})$ (где: L – «Низкая» = 0,77; H – «Высокая» = 0,44); $\boldsymbol{PR}_{uz}$ – соответствие полномочиям, которое представляется множеством $\boldsymbol{PR}_{uz}=\{\bigcup_{pr=1}^{3} PR_{uz,pr}\}=\{PR_{uz,1}, PR_{uz,2},\ \ PR_{uz,3}\}=\ \ \{N, L, H\}$, $(uz=\overline{1,n_{rs}},\ \ pr=\overline{1,3})$ (где: N – «Отсутствует» = 0,85; L – «Низкое» $=\begin{cases}0,62\ при\ S_{uz,1}=U,\\0,68\ при\ S_{uz,2}=C,\end{cases}$ при этом $\boldsymbol{S}_{uz}$ – область действия, можно представить в виде множества $\boldsymbol{S}_{uz}=\{\bigcup_{s=1}^{2} S_{uz,s}\}=\{S_{uz,1}, S_{uz,2}\}=\{U, C\}$, $(uz=\overline{1,n_{rs}},\ s=\overline{1,2})$, (где: U – «Без изменений»; C – «Изменяется»); H – «Высокое» $=\begin{cases}0,27\ при\ S_{uz,1}=U,\\0,50\ при\ S_{uz,2}=C\end{cases}$); $\boldsymbol{UI}_{uz}$ – взаимодействие с пользователем, представляемое множеством $\boldsymbol{UI}_{uz}=\{\bigcup_{ui=1}^{2} UI_{uz,ui}\}=\{UI_{uz,1}, UI_{uz,2}\}=\{N, R\}$, $(uz=\overline{1,n_{rs}},\ ui=\overline{1,2})$ (где: N – «Не требуется» = 0,85; R –

«Требуется» = 0,62); $\boldsymbol{C}_{uz}$ – воздействие на конфиденциальность, определяемое в виде множества $\boldsymbol{C}_{uz} = \{\bigcup_{c=1}^{3} C_{uz,c}\} = \{C_{uz,1}, C_{uz,2}, C_{uz,3}\} = \{N, L, H\}$, $(uz = \overline{1, n_{rs}}$, $c = \overline{1,3})$, (где: N – «Отсутствующее» = 0; L – «Низкое» = 0,22; H – «Высокое» = 0,56); $\boldsymbol{I}_{uz}$ – воздействие на целостность, которое представляется множеством $\boldsymbol{I}_{uz} = \{\bigcup_{in=1}^{3} I_{uz,in}\} = \{I_{uz,1}, I_{uz,2}, I_{uz,3}\} = \{N, L, H\}$, $(uz = \overline{1, n_{rs}}$, $in = \overline{1,3})$, (где: N – «Отсутствующее» = 0; L – «Низкое» = 0,22; H – «Высокое» = 0,56); $\boldsymbol{A}_{uz}$ – воздействие на доступность, которое может представляться множеством $\boldsymbol{A}_{uz} = \{\bigcup_{ai=1}^{3} A_{uz,ai}\} = \{A_{uz,1}, A_{uz,2}, A_{uz,3}\} = \{N, L, H\}$, $(uz = \overline{1, n_{rs}}$, $ai = \overline{1,3})$, (где: N – «Отсутствующее» = 0; L – «Низкое» = 0,22; H – «Высокое» = 0,56);

$\boldsymbol{T}$ – временные (Temporal) оценки, представленные в виде множества $\boldsymbol{T} = \{\bigcup_{uz=1}^{n_{rs}} T_{uz}\}$, $(uz = \overline{1, n_{rs}})$, члены которого определяются посредством группы множеств параметров: $\boldsymbol{EX}_{uz}$, $\boldsymbol{RL}_{uz}$, $\boldsymbol{RC}_{uz}$, $(uz = \overline{1, n_{rs}})$, где $\boldsymbol{EX}_{uz}$ – возможность использования, которая может представляться как множество $\boldsymbol{EX}_{uz} = \{\bigcup_{ex=1}^{5} EX_{uz,ex}\} = \{EX_{uz,1}, ..., EX_{uz,5}\} = \{X, U, POC, F, H\}$, $(uz = \overline{1, n_{rs}}$, $ex = \overline{1,5})$, (где: X – «Нет данных» = 1; U – «Теоретическая (нет доказательств)» = 0,91; POC – «Экспериментальная» = 0,94; F – «Функциональная» = 0,97; H – «Высокая» = 1); $\boldsymbol{RL}_{uz}$ – уровень исправления (показатель степени готовности решения), определяемый в виде множества $\boldsymbol{RL}_{uz} = \{\bigcup_{rl=1}^{5} RL_{uz,rl}\} = \{RL_{uz,1}, ..., RL_{uz,5}\} = \{X, OF, TF, W, U\}$, $(uz = \overline{1, n_{rs}}$, $rl = \overline{1,5})$, (где: X – «Нет данных» = 1; OF – «Официальный патч» = 0,95; TF – «Временное решение» = 0,96; W – «Решение на основе советов и рекомендаций» = 0,97; U – «Отсутствующий» = 1); $\boldsymbol{RC}_{uz}$ – достоверность отчета (показатель степени достоверности информации), которая представляется множеством $\boldsymbol{RC}_{uz} = \{\bigcup_{rc=1}^{4} RC_{uz,rc}\} = \{RC_{uz,1}, ..., RC_{uz,4}\} = \{X, U, R, C\}$, $(uz = \overline{1, n_{rs}}$, $rc = \overline{1,4})$, (где: X – «Нет данных» = 1; U – «Неопределенна» = 0,92; R – «Обоснованная» = 0,96; C – «Подтверждена» = 1);

$\boldsymbol{E}$ – метрики среды окружения (Environmental), представляемые в виде множества $\boldsymbol{E} = \{\bigcup_{uz=1}^{n_{rs}} E_{uz}\}$, $(uz = \overline{1, n_{rs}})$, члены которого определяются посредством группы множеств параметров: $\boldsymbol{CR}_{uz}$, $\boldsymbol{IR}_{uz}$, $\boldsymbol{AR}_{uz}$, $\boldsymbol{MS}_{uz}$, $\boldsymbol{MAV}_{uz}$, $\boldsymbol{MAC}_{uz}$, $\boldsymbol{MPR}_{uz}$, $\boldsymbol{MUI}_{uz}$, $\boldsymbol{MC}_{uz}$, $\boldsymbol{MI}_{uz}$, $\boldsymbol{MA}_{uz}$, $(uz = \overline{1, n_{rs}})$, где $\boldsymbol{CR}_{uz}$ – требования к конфиденциальности, определяемые в виде множества $\boldsymbol{CR}_{uz} = \{\bigcup_{cr=1}^{4} CR_{uz,cr}\} = \{CR_{uz,1}, ..., CR_{uz,4}\} = \{X, L, M, H\}$, $(uz = \overline{1, n_{rs}}$, $cr = \overline{1,4})$, (где: X – «Неопределенные» = 1; L – «Низкие» = 0,5; M – «Средние» = 1; H – «Высокие» = 1,5); $\boldsymbol{IR}_{uz}$ – требования к целостности, представляемые множеством $\boldsymbol{IR}_{uz} = \{\bigcup_{ir=1}^{4} IR_{uz,ir}\} = \{IR_{uz,1}, ..., IR_{uz,4}\} = \{X, L, M, H\}$, $(uz = \overline{1, n_{rs}}$, $ir = \overline{1,4})$, (где: X – «Неопределённые» = 1; L – «Низкие» = 0,5; M – «Средние» = 1; H – «Высокие» = 1,5); $\boldsymbol{AR}_{uz}$ – требования к доступности, которые представляются в виде множества $\boldsymbol{AR}_{uz} = \{\bigcup_{ar=1}^{4} AR_{uz,ar}\} = \{AR_{uz,1}, ..., AR_{uz,4}\} = \{X, L, M, H\}$, $(uz = \overline{1, n_{rs}}$, $ar = \overline{1,4})$, (где: X – «Неопределённые» = 1; L – «Низкие» = 0,5; M – «Средние» = 1; H – «Высокие» = 1,5); $\boldsymbol{MS}_{uz}$ – модифицированная область действия, которую можно представить в виде множества $\boldsymbol{MS}_{uz} = \{\bigcup_{ms=1}^{3} MS_{uz,ms}\} = \{MS_{uz,1}, MS_{uz,2}, MS_{uz,3}\} = \{X, U, C\}$, $(uz = \overline{1, n_{rs}}, ms = \overline{1,3})$, (где: X – «Неопределённа»; U – «Без изменений»; C – «Изменяется»);. $\boldsymbol{MAV}_{uz}$ – модифицированный вектор кибератаки, который представляется в виде множества $\boldsymbol{MAV}_{uz} = \{\bigcup_{mav=1}^{5} MAV_{uz,mav}\} = \{MAV_{uz,1}, ..., MAV_{uz,5}\} = \{X, N, A, L, P\}$, $(uz = \overline{1, n_{rs}}, mav = \overline{1,5})$, (где: X – «Неопределённый» = 1; N – «Сеть» = 0,85; A – «Сопряженная сеть» = 0,62; L – «Локальный доступ» = 0,55; P – «Физический доступ» = 0,2); $\boldsymbol{MAC}_{uz}$ – модифицированная сложность кибератаки, представляемая множеством $\boldsymbol{MAC}_{uz} = \{\bigcup_{mac=1}^{3} MAC_{uz,mac}\} = \{MAC_{uz,1}, MAC_{uz,2}, MAC_{uz,3}\} = \{X, L, H\}$, $(uz = \overline{1, n_{rs}}, mac = \overline{1,3})$, (где: X – «Неопределенная» = 1; L – «Низкая» = 0,77; H – «Высокая» = 0,44); $\boldsymbol{MPR}_{uz}$ – модифицированное соответствие полномочиям, которое представляется множеством $\boldsymbol{MPR}_{uz} = \{\bigcup_{mpr=1}^{4} MPR_{uz,mpr}\} = \{MPR_{uz,1}, MPR_{uz,2}, MPR_{uz,3}, MPR_{uz,4}\} = \{X, N, L, H\}$, $(uz = \overline{1, n_{rs}}$, $mpr = \overline{1,4})$, (где: X – «Неопределенно» = 1; N – «Отсутствует» = 0,85; L – «Низкое» $= \begin{cases} 0,62 \text{ при } MS_{uz,1} = U, \\ 0,68 \text{ при } MS_{uz,2} = C; \end{cases}$ H – «Высокое» $= \begin{cases} 0,27 \text{ при } MS_{uz,1} = U, \\ 0,50 \text{ при } MS_{uz,2} = C \end{cases}$); $\boldsymbol{MUI}_{uz}$ – модифицированное взаимодействие с пользователем, представляемое множеством $\boldsymbol{MUI}_{uz} = \{\bigcup_{mui=1}^{3} MUI_{uz,mui}\} = \{MUI_{uz,1}, MUI_{uz,2}, MUI_{uz,3}\} = \{X, N, R\}$, $(uz = \overline{1, n_{rs}}, mui = \overline{1,2})$, (где: X – «Неопределенное» = 1; N – «Не требуется» = 0,85; R – «Требуется» = 0,62); $\boldsymbol{MC}_{uz}$ – модифицированное воздействие на конфиденциальность, определяемое в виде множества $\boldsymbol{MC}_{uz} = \{\bigcup_{mc=1}^{4} MC_{uz,mc}\} =$

$\{MC_{uz,1}, MC_{uz,2}, MC_{uz,3}, MC_{uz,4}\} = \{X, N, L, H\}$, $(uz = \overline{1, n_{rs}}$, $mc = \overline{1,4})$, (где: X – «Неопределенное» = 1; N – «Отсутствующее» = 0; L – «Низкое» = 0,22; H – «Высокое» = 0,56); $\boldsymbol{MI}_{uz}$ – модифицированное воздействие на целостность, которое представляется множеством $\boldsymbol{MI}_{uz} = \{\bigcup_{min=1}^{4} MI_{uz,min}\} = \{MI_{uz,1}, MI_{uz,2}, MI_{uz,3}, MI_{uz,4}\} = \{X, N, L, H\}$, $(uz = \overline{1, n_{rs}}$, $min = \overline{1,4})$, (где: X – «Неопределенное» = 1; N – «Отсутствующее» = 0; L – «Низкое» = 0,22; H – «Высокое» = 0,56); $\boldsymbol{MA}_{uz}$ – модифицированное воздействие на доступность, которое может представляться множеством $\boldsymbol{MA}_{uz} = \{\bigcup_{mai=1}^{4} MA_{uz,mai}\} = \{MA_{uz,1}, MA_{uz,2}, MA_{uz,3}, MA_{uz,4}\} = \{X, N, L, H\}$, $(uz = \overline{1, n_{rs}}$, $mai = \overline{1,4})$, (где: X – «Неопределенное» = 1; N – «Отсутствующее» = 0; L – «Низкое» = 0,22; H – «Высокое» = 0,56);

Далее введем ЛП «УРОВЕНЬ ОЦЕНОЧНОГО ПАРАМЕТРА $\boldsymbol{EP}_i$» ($\boldsymbol{K}_{EP_i}$), которая определяется кортежем [2-6] < $\boldsymbol{K}_{EP_i}$, $\underset{\sim}{T}_{K_{EP_i}}$, $\boldsymbol{X}_{EP_i}$ >, где базовые терм-множества задаются m термами $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{K_{EP_i j}}$. Для $\underset{\sim}{T}_{K_{EP_i 1}}$, $\underset{\sim}{T}_{K_{EP_i 2}}$,…, $\underset{\sim}{T}_{K_{EP_i j-1}}$, $\underset{\sim}{T}_{K_{EP_i j}}$, …, $\underset{\sim}{T}_{K_{EP_i m}}$, для которых соответственно определяют свои интервалы значений по каждому $\boldsymbol{EP}_i$, $(i = \overline{1, g})$ – $[k_{EP_i 1}; k_{EP_i 2}[$, $[k_{EP_i 2}; k_{EP_i 3}[$, …, $[k_{EP_i j-1}; k_{EP_i j}[$, $[k_{EP_i j}; k_{EP_i j+1}[$, …, $[k_{EP_i m}; k_{EP_i m+1}]$. С целью удобства отображения оценочных параметров через интервалы допустимых значений воспользуемся табл. 1.

Далее с помощью соответствующего метода [9], который реализуется посредством четырех этапов осуществим преобразование интервалов в нечеткие числа (НЧ) – $\underset{\sim}{T}_{K_{EP_i j}} = (ai_j; bi_{1j}; bi_{2j}; ci_j)$. Для этого посредством следующих переопределений модифицируем выражение (5) метода [9]: $a_j = b_{2j}$, $c_j = b_{1j}$, (где $j = \overline{1, m}$, а m – количество терм-множеств), $a_1 = b_{11} = 0$ и $c_m = b_{2m} = k_{m+1}$.

Оценка значимости $\boldsymbol{EP}_i$ выполняется с помощью параметров из множества $\boldsymbol{LS} \in \{LS_i\}$, $(i = \overline{1, g})$, а оценка текущего значения оценочного параметра – с помощью множества $\boldsymbol{ep} \in \{ep_{uz,i}\}$, $(uz = \overline{1, n_{rs}}, i = \overline{1, g})$.

Определение значений НЧ оценочных параметров Таблица 1

$\boldsymbol{EP}_i$	НЧ $\underset{\sim}{T}_{K_{EP_i j}} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$ для $\underset{\sim}{T}_{K_{EP_i 1}}$ – $\underset{\sim}{T}_{K_{EP_i m}}$, $(j = \overline{1, m})$				
	$\underset{\sim}{T}_{K_{EP_i 1}}$	…	$\underset{\sim}{T}_{K_{EP_i j}}$	…	$\underset{\sim}{T}_{K_{EP_i m}}$
$\boldsymbol{EP}_1$	$(a1_1; b1_{11}; b1_{21}; c1_1)$	…	$(a1_j; b1_{1j}; b1_{2j}; c1_j)$	…	$(a1_m; b1_{1m}; b1_{2m}; c1_m)$
…	…	…	…	…	…
$\boldsymbol{EP}_i$	$(ai_1; bi_{11}; bi_{21}; ci_1)$	…	$(ai_j; bi_{1j}; bi_{2j}; ci_j)$	…	$(ai_m; bi_{1m}; bi_{2m}; ci_m)$
…	…	…	…	…	…
$\boldsymbol{EP}_g$	$(ag_1; bg_{11}; bg_{21}; cg_1)$	…	$(ag_j; bg_{1j}; bg_{2j}; cg_j)$	…	$(ag_m; bg_{1m}; bg_{2m}; cg_m)$

Шаг 4 (Определение количества терм-множеств), Шаг 5 (Оценка уровня значимости оценочных параметров) и **Шаг 6 (Определение эталонных значений степени риска)** – аналогичны методу описанному в [9].

Шаг 7 (Определение эталонных значений оценочных параметров). Здесь экспертами производится определение эталонных значений для ЛП $\boldsymbol{K}_{EP_i}$, т.е. задается количество термов в терм-множестве $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}}$.

Для преобразования интервалов в НЧ воспользуемся предложенным в [9] методом, который реализуется посредством четырех этапов, с учетом модификации выражения (5) из [9] описанной на шаге 3. Для удобства отображения оценочных параметров через НЧ используем табл. 1.

Например, если $\boldsymbol{EP}_i$ представляются трапециевидными НЧ с функциями принадлежности (ФП) $\mu_1(ep_{uz,i})$, …, $\mu_j(ep_{uz,i})$, …, $\mu_m(ep_{uz,i})$, то они соответственно вычисляются по выражению (4) из [6], с помощью которого для интервалов $\boldsymbol{EP}_i$ можно сформировать значения $\mu_j(ep_{uz,i})$.

Шаг 8 (Оценка текущих значений параметров). На этом шаге по каждому оценочному параметру $\{\bigcup_{i=1}^{3} \boldsymbol{EP}_i\} = \{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_3\} = \{\boldsymbol{B}, \boldsymbol{T}, \boldsymbol{E}\}$, $(i = \overline{1,3})$ определяются $ep_{uz,i}$ $\forall V_{rs,uz}$, $(rs = \overline{1, ro}, uz = \overline{1, n_{rs}})$, т.е. $\{ep_{uz,i}\} = \{ep_{uz,\boldsymbol{B}}, ep_{uz,\boldsymbol{T}}, ep_{uz,\boldsymbol{E}}\}$. Значения каждого из параметров, можно взять из известных баз данных [15] или определить по соответствующим формулам [14]:

$$B_{uz} = \begin{cases} 0 \ \ при\ IM_{uz} \le 0, \\ roundUp_1(\min[(IM_{uz} + EXb_{uz}), 10])\ при\ S_{uz,1} = U, \\ roundUp_1(\min[1,08 \cdot (IM_{uz} + EXb_{uz}), 10])\ при\ S_{uz,2} = C, \end{cases}$$

где $roundUp_1(\,)$ – функция округления до первого знака после запятой (например, 3,822 будет округлена до 3,8);

$$IM_{uz} = \begin{cases} 6,42ISC_{uz} \text{ при } S_{uz,1} = U, \\ 7,52(ISC_{uz} - 0,029) - 3,25(ISC_{uz} - 0,02)^{15} \text{ при } S_{uz,2} = C, \end{cases}$$

где $ISC_{uz} = 1 - ((1 - C_{uz,c})(1 - I_{uz,in})(1 - A_{uz,ai}))$, значения $S_{uz,s}$, $C_{uz,c}$, $I_{uz,in}$, $A_{uz,ai}$ берутся из шага 3 этого метода, а $EXb_{uz} = 8,22AV_{uz,av} \cdot AC_{uz,ac} \cdot PR_{uz,pr} \cdot UI_{uz,ui}$;

$$E_{uz} = \begin{cases} 0 \text{ при } MIM_{uz} \le 0, \\ roundUp_1(\min[(MIM_{uz} + MEXb_{uz})EX_{uz,ex} \cdot RL_{uz,rl} \cdot RC_{uz,rc}, 10]) \text{ при } MS_{uz,1} = U, \\ roundUp_1(\min[1,08(MIM_{uz} + MEXb_{uz})EX_{uz} \cdot RL_{uz,rl} \cdot RC_{uz,rc}, 10]) \text{ при } MS_{uz,1} = C, \end{cases}$$

где

$$MIM_{uz} = \begin{cases} 6,42(MISC_{uz}) \text{ при } MS_{uz,1} = U, \\ 7,52(MISC_{uz} - 0,029) - 3,25(MISC_{uz} - 0,02)^{15} \text{ при } MS_{uz,2} = C, \end{cases}$$

а $MEXb_{uz} = 8,22MAV_{uz,mav} \cdot MAC_{uz,mac} \cdot MPR_{uz,mpr} \cdot MUI_{uz,mui}$ и $MISC_{uz} = \min[(1 - (1 - MC_{uz,mc} \cdot CR_{uz,cr})\ (1 - MI_{uz,min} \cdot IR_{uz,ir})\ (1 - MA_{uz,mai} \cdot AR_{uz,ar})),\ 0,915]$, при этом значения $MS_{uz,ms}$, $MAV_{uz,mav}$, $MAC_{uz,mac}$, $MPR_{uz,mpr}$, $MUI_{uz,mui}$, $MC_{uz,mc}$, $CR_{uz,cr}$, $MI_{uz,min}$, $IR_{uz,ir}$, $MA_{uz,mai}$, $AR_{uz,ar}$ уже определены на шаге 3 данного метода. Здесь E_{uz} является корректирующим оценочным параметром, который переопределяет B_{uz} и T_{uz}.

Шаг 9 (Классификация текущих значений), Шаг 10 (Оценка степени риска) и **Шаг 11 (Формирование структурированного параметра риска)** аналогичны методу в [6].

Рассмотрим работу предложенного метода на конкретном примере.

Пример 1

Шаг 1. На первом шаге определяются полные множества всех РИС и уязвимостей, при $r = r_{BD}$ и $n = n_{NVD}$, т.е. $\boldsymbol{RIS} = \{\bigcup_{rs=1}^{r} RIS_{rs}\}$, $(rs = \overline{1,r})$ и $\boldsymbol{V} = \{\bigcup_{uz=1}^{n} V_{uz}\}$, $(uz = \overline{1,n})$, где r_{BD} и n_{NVD} – количество всех РИС (например, в государственных или частных БД) и уязвимостей (например, в NVD [15]) соответственно.

$$T_{uz} = roundUp_1(B_{uz} \cdot EX_{uz,ex} \cdot RL_{uz,rl} \cdot RC_{uz,rc}),$$ где значения $EX_{uz,ex}$, $RL_{uz,rl}$ и $RC_{uz,rc}$ также берутся из шага 3 метода.

Шаг 2. На этом шаге с помощью множества $\boldsymbol{RIS}$ автоматически (посредством перебора данных соответствующих баз) или экспертным путем определяется содержимое $\boldsymbol{RISO}$ для конкретного объекта оценивания, например, при ro = 5 $\exists \boldsymbol{RISO} = \{\bigcup_{rs=1}^{5} RISO_{rs}\} = \{RISO_1, ..., RISO_5\}$, $(rs = \overline{1,5})$, где, например, $RISO_1$ = «Файловый сервер», $RISO_2$ = «Банк данных», $RISO_3$ = «Архив данных», $RISO_4$ = «Маршрутизатор», $RISO_5$ = «Web-сервер.

Далее относительно $\boldsymbol{RISO}$, например, при n_1 = 5, n_2 = 5, n_3 = 7, n_5 = 4, n_6 = 2, автоматически или экспертным путем посредством NVD [15] идентифицируются следующие уязвимости –

$$\{\bigcup_{rs=1}^{5} \boldsymbol{V}_{rs}\} = \{\bigcup_{rs=1}^{5} \{\bigcup_{uz=1}^{n_{rs}} V_{rs,uz}\} = \{\{V_{1,1}, V_{1,2}, V_{1,3}, V_{1,4}, V_{1,5}\}, \{V_{2,1}, V_{2,2}, V_{2,3}, V_{2,4}, V_{2,5}\},$$
$$\{V_{3,1}, V_{3,2}, V_{3,3}, V_{3,4}, V_{3,5}, V_{3,6}, V_{3,7}\}, \{V_{4,1}, V_{4,2}, V_{4,3}, V_{4,4}\}, \{V_{5,1}, V_{5,2}\}\}.$$

Далее, например, при $rs = 2$ реализуем ОР для $RISO_2$, по которому экспертами идентифицированы следующие уязвимости:

$V_{2,1}$ = «CVE-2016-5849» – уязвимость Siemens SICAM PAS до версии 8.07 позволяет локальным пользователям получить доступ к конфиденциальной информации о конфигурации за счет использования события остановки базы данных. Оценка CVSS Severity (v2) = 1,9 (LOW) и (v3) = 2,5 (LOW);

$V_{2,2}$ = «CVE-2016-5703» – уязвимость SQL инъекций в библиотеках/центральных столбцах (.lib.php) в PhpMyAdmin версий 4.4.x ÷ 4.4.15.7 и 4.6.x ÷ 4.6.3 позволяет удаленному злоумышленнику выполнить произвольные команды SQL с помощью созданного имени базы данных, используя ошибку в запросе центрального столбца. Оценка CVSS Severity (v2) = 7,5 (HIGH) и (v3) = 9,8 (CRITICAL);

$V_{2,3}$ = «CVE-2016-0298» – уязвимость обхода каталогов в IBM Security Guardium Database Activity Monitor версий 10 ÷ 10.0p100 позволяет осуществлять удаленным пользователям проверку подлинности и читать произвольные файлы с помощью сформированного URL. Оценка CVSS Severity (v2) = 4,0 (MEDIUM) и (v3) = 6,5 (MEDIUM);

$V_{2,4}$ = «CVE-2016-5705» – уязвимость множественного межсайтового скриптинга (XSS) в PhpMyAdmin версий 4.4.x ÷ 4.4.15.7 и 4.6.x ÷ 4.6.3 позволяет удаленному злоумышленнику внедрить произвольный веб-скрипт или HTML с помощью векторов, включающих поля: (1) данные сервера-привилегий – сертификат об привилегиях пользователя страницы, (2) сообщения об ошибках «недействительные JSON» в консоли ошибок, (3) имя базы данных, (4) имя группы. Оценка CVSS Severity (v2) = 4,3 (MEDIUM) и (v3) = 6,1 (MEDIUM);

$V_{2,5}$ = «CVE-2016-4328» – уязвимость предоперационной системы управления информацией MEDHOST (так называемой PIMS или VPIMS) до 2015R1 имеет четко прописанные учетные данные, что делает ее более доступной для удаленного злоумышленника при получении доступа к конфиденциальной информации с помощью прямых запросов к серверу базы данных приложений. Оценка CVSS Severity (v2) = 10 (HIGH) и (v2) = 9,8 (CRITICAL).

Шаг 3. Здесь, например, определим множество параметров ОР при ro = 2 (т.е. для LR_2) и при $n_2 = 5$ (т.е. для $\{\bigcup_{uz=1}^{5} LRV_{2,uz}\} = \{LRV_{2,1}, LRV_{2,2}, LRV_{2,3}, LRV_{2,4}, LRV_{2,5}\}$). Отображение результатов ОР для LR_2 и $LRV_{2,uz}$, $(uz = \overline{1,5})$ при m = 5 выполним посредством термов $\bigcup_{j=1}^{5} \tilde{T}^{DR_j}$ = {«Незначительный риск нарушения ИБ» (НР), «Степень риска нарушения ИБ низкая» (РН), «Степень риска нарушения ИБ средняя» (РС), «Степень риска нарушения ИБ высокая» (РВ), «Предельный риск нарушения ИБ» (ПР)}, которые могут быть отображены на универсальное множество $\boldsymbol{X}_{DR} \in \{0, max_{DR}\}$. В последствии для каждого $\tilde{T}^{DR_1}$, $\tilde{T}^{DR_2}$, $\tilde{T}^{DR_3}$, $\tilde{T}^{DR_4}$, $\tilde{T}^{DR_5}$ определяются интервалы с использованием модифицированной шкалы Харрингтона [2, 5, 6], т.е. $[dr_1; dr_2[$, $[dr_2; dr_3[$, $[dr_3; dr_4[$, $[dr_4; dr_5[$ и $[dr_5; dr_6]$ будут соответственно принимать значения [0; 20[, [20; 40[, [40; 60[, [60; 80[и [80; 100].

Далее воспользуемся множеством оценочных параметров $\boldsymbol{EP} = \{\boldsymbol{B}, \boldsymbol{T}, \boldsymbol{E}\}$. Зададим для ЛП $\boldsymbol{K}_{EP_i}$ при m = 5 следующие термы – $\bigcup_{j=1}^{5} \tilde{T}_{K_{EP_ij}}$ = {«Отсутствует» (N), «Низкий» (L), «Средний» (M), «Высокий» (H), «Критический» (C)}, которые в лингвистической форме характеризуют уровень оценочного параметра и могут быть отображены на универсальное множество $\boldsymbol{X}_{EP_i} \in \{0, \max_{K_{EP_i}}\}$. Далее для каждого терма $\tilde{T}_{K_{EP_i1}}$, $\tilde{T}_{K_{EP_i2}}$, $\tilde{T}_{K_{EP_i3}}$, $\tilde{T}_{K_{EP_i4}}$, $\tilde{T}_{K_{EP_i5}}$ оценочных параметров [2-6] определим интервалы $[k_{EP_i1}; k_{EP_i2}[$, $[k_{EP_i2}; k_{EP_i3}[$, $[k_{EP_i3}; k_{EP_i4}[$, $[k_{EP_i4}; k_{EP_i5}[$, $[k_{EP_i5}; k_{EP_i6}]$, которым будут соответствовать значения [2, 5, 6, 14] – [0; 0,1[, [0,1; 4[, [4; 7[, [7; 9[, [9; 10].

Шаг 4. Определим количество необходимых терм-множеств для ОР ЛП $\boldsymbol{DR}^{(m)}$ и $\boldsymbol{K}_{EP_i}^{(m)}$, при m = 5 (см. табл. 2 и 3 соответственно). В случае необходимости можем с помощью методов, описанных в [7, 8] реализовать инкрементирование или декрементирование соответствующих терм-множеств.

Определение эталонных значений НЧ степени риска (пример) Таблица 2

ЛП	НЧ $\underset{\sim}{X}_{DR_j} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$ для $\tilde{T}^{DR_1} \div \tilde{T}^{DR_5}$, $(j = \overline{1,5})$				
	$\tilde{T}^{DR_1}$ $(a_1; b_{11}; b_{21}; c_1)$	$\tilde{T}^{DR_2}$ $(a_2; b_{12}; b_{22}; c_2)$	$\tilde{T}^{DR_3}$ $(a_3; b_{13}; b_{23}; c_3)$	$\tilde{T}^{DR_4}$ $(a_4; b_{14}; b_{24}; c_4)$	$\tilde{T}^{DR_5}$ $(a_5; b_{15}; b_{25}; c_5)$
DR	(0;0; 11,11; 22,22)	(11,11; 22,22; 33,33; 44,44)	(33,33; 44,44; 55,55; 66,66)	(55,55; 66,66; 77,77; 88,88)	(77,77; 88,88; 100; 100)

Шаг 5. На этом шаге произведем оценку значимости оценочных параметров. Так как для всех оценочных параметров, (например, по мнению экспертов) справедливо отношение порядка $LS_1 \geq LS_2 \geq LS_3$ (см. (1) из [6]), тогда оценку LS осуществим по формуле (2) из [6] т.е.: $LS_1 = 2(g - i + 1)/(g - 1)g = 2(3 - 1 + 1)/(3 - 1)3 = 1$; $LS_2 = 2(3 - 2 + 1)/(3 - 1)3 = 0{,}67$; $LS_3 = 2(3 - 3 + 1)/(3 - 1)3 = 0{,}33$, $(i = \overline{1,3})$.

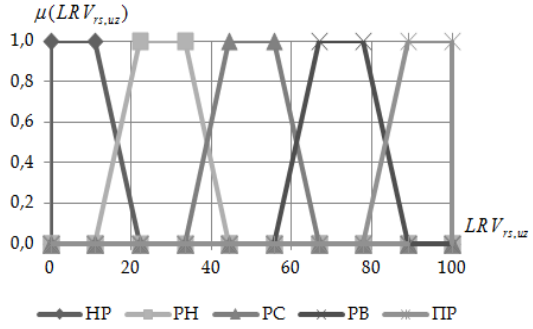

Рис. 1. Пример эталонных НЧ для ЛП **DR**

Шаг 6. Здесь определим эталонные значения для ЛП **DR**. С помощью выражений (1)–(5) из [9] представим для $\tilde{T}^{DR_j} = (a_j; b_{1j}; b_{2j}; c_j)$ числовые значения, которые заносятся в таблицу 2. Их графическая интерпретация отображена на рис. 1.

Шаг 7. Далее определим эталонные значения для ЛП $\boldsymbol{K}_{EP_i}$. Преобразование интервалов в НЧ $\tilde{T}_{K_{EP_ij}} = (ai_j; bi_{1j}; bi_{2j}; ci_j)$ реализуем с помощью четырех этапов предложенного в [9] метода и поправок, принятых на шаге 3.

Этапы 1 и 3 аналогичны примеру приведенному в [6].

Этап 4. На этом этапе реализуем нормирование результатов по выражению (5) из [9] с учетом модификации: $bi_{i11} = (b''_{i11} \cdot k_{EP_i6})/b''_{i25} = 0$; $bi_{i21} = (b''_{i21} \cdot k_{EP_i6})/b''_{i25} = 0{,}051$ и т.д., $a_{i_2} = bi_{21}$, $a_{i_3} = bi_{22}$, $a_{i_4} = bi_{23}$, $a_{i_5} = bi_{24}$, $c_{i_1} = bi_{12}$, $c_{i_2} = bi_{13}$, $c_{i_3} = bi_{14}$, $c_{i_4} = bi_{15}$. Далее, согласно той же формуле (5) $a_{i_1} = bi_{11} = 0$, а $c_{i_5} = bi_{25} = 10$. Все полученные в результате вычисления значения занесены в табл. 3, а их графическая интерпретация отображена на рис. 2.

Шаг 8. Текущее состояние $RISO_2$ характеризуется значениями оценочных параметров $ep_{uz,i}$ $\forall V_{rs,uz}$, которые определяются с помощью оценок

CVSS *версии 3*, представленных на сайте NVD [15]. Поскольку не всегда все значения оценочных параметров по уязвимостям присутствуют в базе NVD, то для получения недостающих воспользуемся формулами из шага 7.

Определение эталонных значений НЧ оценочных параметров (пример) Таблица 3

EP_i	НЧ $\underset{\sim}{T}_{K_{EP_ij}} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$ для $\underset{\sim}{T}_{K_{EP_i1}} \div \underset{\sim}{T}_{K_{EP_i5}}$, ($j=\overline{1,5}$, $i=\overline{1,g}$)				
	$\underset{\sim}{T}_{K_{EP_i1}}$ (ai_1; bi_{11}; bi_{21}; ci_1)	$\underset{\sim}{T}_{K_{EP_i2}}$ (ai_2; bi_{12}; bi_{22}; ci_2)	$\underset{\sim}{T}_{K_{EP_i3}}$ (ai_3; bi_{13}; bi_{23}; ci_3)	$\underset{\sim}{T}_{K_{EP_i4}}$ (ai_4; bi_{14}; bi_{24}; ci_4)	$\underset{\sim}{T}_{K_{EP_i5}}$ (ai_5; bi_{15}; bi_{25}; ci_5)
B, T, E	(0;0;0,1;1,1)	(0,1;1,1;3,1;4,9)	(3,1;4,9;6,4;7,7)	(6,4;7,7;8,7;9,5)	(8,7;9,5;10;10)

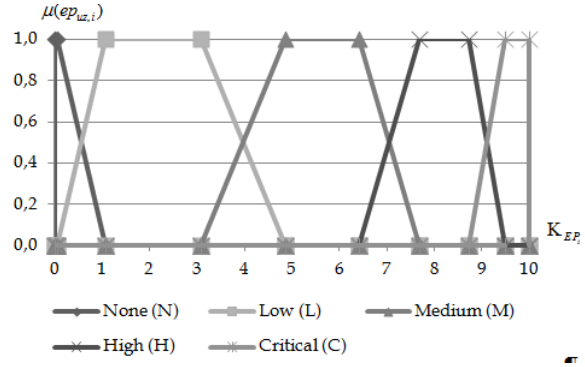

Рис. 2. Пример эталонных НЧ для оценочных параметров B_{uz}, T_{uz}, E_{uz}, ($uz=\overline{1,5}$)

Расчет для $V_{2,1}$ = «CVE-2016-5849»:

– для B_1, исходя из того, что величинам $AV_{1,3}$, $AC_{1,2}$, $PR_{1,2}$, $S_{1,1}$, $UI_{1,1}$, $C_{1,2}$, $I_{1,1}$ и $A_{1,1}$ соответствуют определенные значения «*L*», «*H*», «*L*», «*U*», «*N*», «*L*», «*N*» и «*N*», то $AV_{1,3}$ = 0,55, $AC_{1,2}$ = 0,44, $PR_{1,2}$ = 0,62, $UI_{1,1}$ =0,85, $C_{1,2}$ = 0,22, $I_{1,1}$ = 0 и $A_{1,1}$ = 0. На основе этого вычисляем $ISC_1 = 1-((1-C_{1,2})(1-I_{1,1})(1-A_{1,1}))$ = 1 – ((1 – 0,22)(1 – 0)(1 – 0)) = 0,22, $IM_1 = 6{,}42 \cdot ISC_1$ = 1,4124, $EXb_1 = 8{,}22\, AV_{1,3} \cdot AC_{1,2} \cdot PR_{1,2} \cdot UI_{1,1}$ = 8,22 · 0,55 · 0,44 · 0,62 · 0,85 = 1,0483, а $B_1 = roundUp_1[\min(IM_1 + EXb_1),10]$ = $roundUp_1$ [min(1,4124 + 1,0483),10] = 2,5;

– для T_1 аналогично B_1 величины и их значения отражены в базе NVD, а в случае отсутствия их значения можно определить, например, экспертным путем, так для $EX_{1,2}$ = «*U*», $RL_{1,2}$ = «*OF*», $RC_{1,4}$ = «*C*» и тогда $EX_{1,2}$ = 0,91, $RL_{1,2}$ = 0,95, $RC_{1,4}$ = 1, а $T_1 = roundUp_1(B_1 \cdot EX_{1,2} \cdot RL_{1,2} \cdot RC_{1,4})$ = $roundUp_1$ (2,5 · 0,91 · 0,95 · 1)=2,2;

– для E_1, по аналогии с T_1, значения также могут быть определены посредством БД или экспертным путем, так, например, если $MAV_{1,4}$ = «L», $MAC_{1,3}$ = «H», $MPR_{1,3}$ = «L», $MUI_{1,2}$ = «N», $MS_{1,2}$ = «U», $MC_{1,3}$ = «L», $MI_{1,2}$ = «N», $MA_{1,2}$ = «N», $CR_{1,3}$ = «M», $IR_{1,2}$ = «L» и $AR_{1,2}$ = «L», тогда $MAV_{1,4}$ =0,55, $MAC_{1,3}$ = 0,44, $MPR_{1,3}$ = 0,62, $MUI_{1,2}$ = 0,85, $MC_{1,3}$ =0,22, $MI_{1,2}$ =0, $MA_{1,2}$ =0, $CR_{1,3}$ = 1, $IR_{1,2}$ = 0,5 и $AR_{1,2}$ = 0,5. На основе этого находим $MISC_1 = \min[(1-(1-MC_{1,3} \cdot CR_{1,3})(1-MI_{1,2} \cdot IR_{1,2})(1-MA_{1,2} \cdot AR_{1,2})), 0{,}915]$ = min[(1 – (1 – 0,22 · 1) (1 – 0 · 0,5) (1 – 0 · 0,5)), 0,915] = 0,22, $MIM_1 = 6{,}42 \cdot MISC_1$ = 6,42 · 0,22 = 1,4124, $MEXb_1 = 8{,}22 MAV_{1,4} \cdot MAC_{1,3} \cdot MPR_{1,3} \cdot MUI_{1,2}$ =8,22 · 0,55 · 0,44 · 0,62 · 0,85 = 1,0483 и E_1 = $roundUp_1(\min[MIM_1 + MEXb_1)EX_{1,1} \cdot RL_{1,1} \cdot RC_{1,4},10])$ = $roundUp_1$ (min[1,4124 + 1,0483) 0,91 · 0,95 · 1, 10]) = 2,2. Полученное значение E_1 скорректировало параметры B_1 и T_1.

Расчет для $V_{2,2}$ = «CVE-2016-5703»:

– для B_2 определены значения $AV_{2,1}$ = «*N*», $AC_{2,1}$ = «*L*», $PR_{2,1}$ = «*N*», $UI_{2,1}$ = «*N*», $S_{2,1}$ = «*U*», $C_{2,3}$ = «*H*», $I_{2,3}$ = «*H*», $A_{2,3}$ = «*H*» и тогда $AV_{2,1}$ = 0,85, $AC_{2,1}$ = 0,77, $PR_{2,1}$ = 0,85, $UI_{2,1}$ = *0,85*, $C_{2,3}$ = $I_{2,3}$ = $A_{2,3}$ = 0,56. Вычисляем ISC_2 = 1 – ((1 – 0,56)(1 – 0,56)(1 – 0,56)) = 0,915, IM_2 = 6,42·0,915 = 5,87, EXb_2 = 8,22·0,85·0,77·0,85·0,85 = 3,89, B_2 = $roundUp_1$ (min[5,87 + 3,89), 10]) = 9,8;

– для T_2 в базе NVD отсутствуют определенные значения, поэтому, например, экспертным путем определим значения для $EX_{2,5}$ = «*H*», $RL_{2,1}$ = «*X*», $RC_{2,1}$ = «UC» и тогда $EX_{2,5}$ = 1, $RL_{2,1}$ = 1, $RC_{2,1}$ = 1, T_2 = $roundUp_1$ (9,8·1·1·1) = 9,8;

– для E_2, по аналогии с T_2, значения определяются также экспертным путем. Если $MAV_{2,2}$ = «N», $MAC_{2,2}$ = «L», $MPR_{2,2}$ = «N», $MUI_{2,2}$ = «N», $MS_{2,2}$ = «U», $MC_{2,4}$ = «H», $MI_{2,4}$ = «H», $MA_{2,4}$ = «H», $CR_{2,4}$ = «H», $IR_{2,4}$ = «H» и $AR_{2,4}$ = «H», тогда $MAV_{2,2}$ =0,85, $MAC_{2,2}$ = 0,77, $MPR_{2,2}$ = 0,85, $MUI_{2,2}$ = 0,85, $MC_{2,4} = MI_{2,4} = MA_{2,4}$ =0,56 и $CR_{2,4}$ = $IR_{2,4}$ = $AR_{2,4}$ = 1,5. На основе этого находим $MISC_2$ = min[(1 – (1 – 0,56 · 1,5) (1 – 0,56 · 1,5) (1 – 0,56 · 1,5)), 0,915] = 0,915, MIM_2 = 6,42 · 0,915 = 5,8743, $MEXb_2$ = 8,22 · 0,85 · 0,77 · 0,85 · 0,85 = 3,887 и E_1 = $roundUp_1$ (min[5,8743 + 3,887) 1 · 1 · 1, 10]) = 9,8. Полученное значение E_2 скорректировало параметры B_2 и T_2.

По аналогии с предыдущими уязвимостями для $V_{2,3}$ = «CVE-2016-0298», $V_{2,4}$ = «CVE-2016-5705»,

$V_{2,5}$ = «CVE-2016-4328» также были сформированы оценочные параметры. Их значения занесены в табл. 4.

Определение текущих значений оценочных параметров (пример 1) Таблица 4

$\boldsymbol{EP}_i$	$ep_{1,i}$	$ep_{2,i}$	$ep_{3,i}$	$ep_{4,i}$	$ep_{5,i}$
B , (i=1)	2,5	9,8	6,5	6,1	9,8
T , (i=2)	2,2	9,8	6	5,4	8,7
E , (i=3)	2,2	9,8	7,7	4,1	8,7

Шаг 9. Далее осуществим классификацию текущих значений $ep_{uz,i}$ по формуле (4) и (5) из [4] при m = 5, результаты которых заносятся в табл. 5:

$$\mu_1(ep_{uz,i})=\begin{cases} L\left(\dfrac{a_{i_1}-ep_{uz,i}}{a_{i_1}-b_{i_{11}}}\right), & ep_{uz,i}\in[a_{i_1},b_{i_{11}}];\\ 1, & ep_{uz,i}\in[b_{i_{11}},b_{i_{21}}];\\ R\left(\dfrac{ep_{uz,i}-c_{i_1}}{b_{i_{21}}-c_{i_1}}\right), & ep_{uz,i}\in[b_{i_{21}},c_{i_1}], \end{cases}$$

$$\mu_2(ep_{uz,i})=\begin{cases} L\left(\dfrac{a_{i_2}-ep_{uz,i}}{a_{i_2}-b_{i_{12}}}\right), & ep_{uz,i}\in[a_{i_2},b_{i_{12}}];\\ 1, & ep_{uz,i}\in[b_{i_{12}},b_{i_{22}}];\\ R\left(\dfrac{ep_{uz,i}-c_{i_2}}{b_{i_{22}}-c_{i_2}}\right), & ep_{uz,i}\in[b_{i_{22}},c_{i_2}], \end{cases}$$

$$\mu_3(ep_{uz,i})=\begin{cases} L\left(\dfrac{a_{i_3}-ep_{uz,i}}{a_{i_3}-b_{i_{13}}}\right), & ep_{uz,i}\in[a_{i_3},b_{i_{13}}];\\ 1, & ep_{uz,i}\in[b_{i_{13}},b_{i_{23}}];\\ R\left(\dfrac{ep_{uz,i}-c_{i_3}}{b_{i_{23}}-c_{i_3}}\right), & ep_{uz,i}\in[b_{i_{23}},c_{i_3}], \end{cases}$$

$$\mu_4(ep_{uz,i})=\begin{cases} L\left(\dfrac{a_{i_4}-ep_{uz,i}}{a_{i_4}-b_{i_{14}}}\right), & ep_{uz,i}\in[a_{i_4},b_{i_{14}}];\\ 1, & ep_{uz,i}\in[b_{i_{14}},b_{i_{24}}];\\ R\left(\dfrac{ep_{uz,i}-c_{i_4}}{b_{i_{24}}-c_{i_4}}\right), & ep_{uz,i}\in[b_{i_{24}},c_{i_4}], \end{cases}$$

$$\mu_5(ep_{uz,i})=\begin{cases} L\left(\dfrac{a_{i_5}-ep_{uz,i}}{a_{i_5}-b_{i_{15}}}\right), & ep_{uz,i}\in[a_{i_5},b_{i_{15}}];\\ 1, & ep_{uz,i}\in[b_{i_{15}},b_{i_{25}}];\\ R\left(\dfrac{ep_{uz,i}-c_{i_5}}{b_{i_{25}}-c_{i_5}}\right), & ep_{uz,i}\in[b_{i_{25}},c_{i_5}]. \end{cases}$$

Шаг 10. Произведем вычисление показателя степени риска нарушения ИБ по формуле (6) из [6], где m = 5, $j=\overline{1,5}$, $i=\overline{1,3}$, $n_1=\overline{1,5}$, K_{lr_1} =10, K_{lr_2} =30, K_{lr_3} =50, K_{lr_4} =70, K_{lr_5} =90, ks = 0,5 и тогда $LRV_{2,1}$ = 30, $LRV_{2,2}$ = 90, $LRV_{2,3}$ = 54,1, $LRV_{2,4}$ = 48,55, $LRV_{2,5}$ = 80.

Классификация текущих значений оценочных параметров (пример 1) Таблица 5

$\boldsymbol{EP}_i$	Значение $\lambda_{uz,ij}$ для $\{\bigcup_{uz=1}^{5}\boldsymbol{V}_{1,uz}\}$, $(uz=\overline{1,5})$																									
	$\lambda_{1,ij}$ для $\underset{\sim}{T}_{K_{EP_1}}$ ($i=\overline{1,3}$, $j=\overline{1,5}$)					$\lambda_{2,ij}$ для $\underset{\sim}{T}_{K_{EP_2}}$ ($i=\overline{1,3}$, $j=\overline{1,5}$)					$\lambda_{3,ij}$ для $\underset{\sim}{T}_{K_{EP_3}}$ ($i=\overline{1,3}$, $j=\overline{1,5}$)					$\lambda_{4,ij}$ для $\underset{\sim}{T}_{K_{EP_4}}$ ($i=\overline{1,3}$, $j=\overline{1,5}$)					$\lambda_{5,ij}$ для $\underset{\sim}{T}_{K_{EP_5}}$ ($i=\overline{1,3}$, $j=\overline{1,5}$)				
B	0	1	0	0	0	0	0	0	0	1	0	0	0,92	0,08	0	0	0	1	0	0	0	0	0	0	1
T	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	1	0	0	0	0	0	1	0
E	0	1	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0,44	0,56	0	0	0	0	0	1	0

Шаг 11. По аналогии с шагом 8 согласно формуле (4) из [6] вычислим $\mu_j(LRV_{2,uz})$, $(uz=\overline{1,5})$,

$$\mu_j(LRV_{2,uz})=\begin{cases} L\left(\dfrac{a_j-LRV_{2,uz}}{a_j-b_{1j}}\right), & LRV_{2,uz}\in[a_j,b_{1j}];\\ 1, & LRV_{2,uz}\in[b_{1j},b_{2j}];\\ R\left(\dfrac{LRV_{2,uz}-c_j}{b_{2j}-c_j}\right), & LRV_{2,uz}\in[b_{2j},c_j]. \end{cases}$$

Далее с помощью (7) из [6] формируются SP_{uz}:

$SP_1=(LRV_{2,1};\ \underset{\sim}{T}_{DR_2}(\mu_2(LRV_{2,1})))$ = (30; РН), $SP_2=(LRV_{2,2};$

$\underset{\sim}{T}_{DR_5}(\mu_5(LRV_{2,2})))$ = (90; ПР), $SP_3=(LRV_{2,3};\ \underset{\sim}{T}_{DR_3}$

$(\mu_3(LRV_{2,3})))$ = (54,1; РС), $SP_4=(LRV_{2,4};\ \underset{\sim}{T}_{DR_3}$

$(\mu_3(LRV_{2,4})))$ = (48,55; РС), $SP_5=(LRV_{2,5};\ \underset{\sim}{T}_{DR_4}$

$(\mu_4(LRV_{2,5}));\ \underset{\sim}{T}_{DR_5}(\mu_5(DRV_{2,5})))$ = (80; РВ(0,8); РП(0,2)),

где, например, (80; РВ(0,8); ПР(0,2)) словесно интерпретируется, как «Степень риска с числовым эквивалентом 80 граничит между высоким риском и предельным риском по границе РВ – 0,8 и ПР – 0,2».

Также для данного $RISO_2$ на основе выражения (8) из [6], можно вычислить среднее значение степени риска: LR_2 =(30 + 90 + 54,1 + 48,55 + 80) / 5 = 60,53 и сформировать для него SP = (60,53; РС(0,55); РВ(0,45)).

По аналогии с приведенным примеров в [6], для верификации представленного метода осуществим моделирование нескольких состояний среды оценивания: 1-е состояние – уменьшим относительно текущего состояния значения всех оценочных параметров (см. табл. 6 и 7); 2-е состояние – увеличим относительно текущего состояния значения всех оценочных параметров (см. табл. 8 и 9).

Пример 2 (1-е состояние)

Согласно 1-го состояния при m = 5 оценочные параметры принимают значения, которые отражены в табл. 6.

Реализуем классификацию значений $ep_{uz,i}$ по формуле (9) и (10) из [6], результаты которой занесены в табл. 7.

1-е состояние значений оценочных параметров (пример 2) Таблица 6

$\boldsymbol{EP}_i$	$ep_{1,i}$	$ep_{2,i}$	$ep_{3,i}$	$ep_{4,i}$	$ep_{5,i}$
$\boldsymbol{B}$, (i=1)	1,5	8,8	5,5	5,1	8,8
$\boldsymbol{T}$, (i=2)	1,2	8,8	5	4,4	7,7
$\boldsymbol{E}$, (i=3)	1,2	8,8	6,7	3,1	7,7

Произведем вычисление показателя степени риска нарушения ИБ по формуле (6) из [6], где m = 5, $j=\overline{1,5}$, $i=\overline{1,3}$, $n_1=\overline{1,5}$, K_{lr_1} = 10, K_{lr_2} = 30, K_{lr_3} = 50, K_{lr_4} = 70, K_{lr_5} = 90, ks = 0,5 и тогда $LRV_{2,1}$ = 30, $LRV_{2,2}$ = 74, $LRV_{2,3}$ = 50,76, $LRV_{2,4}$ = 44,82, $LRV_{2,5}$ = 72. По формуле (4) из [6] вычислим $\mu_j(LRV_{2,uz})$, $(uz=\overline{1,5})$. С помощью (7) из [6] формируются SP_{uz}: $SP_1=(LRV_{2,1}$; $\underset{\sim}{T}_{DR_2}(\mu_2(LRV_{2,1})))$ = (30; РН), $SP_2=(LRV_{2,2}$; $\underset{\sim}{T}_{DR_4}(\mu_4(DRV_{2,2})))$ = (74; РВ), $SP_3=(LRV_{2,3}$; $\underset{\sim}{T}_{DR_3}(\mu_3(LRV_{2,3})))$ = (50,76; РС), $SP_4=(LRV_{2,4}$; $\underset{\sim}{T}_{DR_3}(\mu_3(LRV_{2,4})))$ = (44,82; РС), $SP_5=(LRV_{2,5}$; $\underset{\sim}{T}_{DR_4}(\mu_4(LRV_{2,5})))$ = (72; РВ).

Далее на основе выражения (8) из [6] для $RISO_2$ можно вычислить среднее значение степени риска, т.е. LR_2 = 54,32 и сформировать для него SP = (54,32; РС).

Классификация 1-го состояния значений оценочных параметров (пример 2) Таблица 7

$\boldsymbol{EP}_i$	Значение $\lambda_{uz,ij}$ для $\{\bigcup_{uz=1}^{5}\boldsymbol{V}_{1,uz}\}$, $(uz=\overline{1,5})$																									
	$\lambda_{1,ij}$ для $\underset{\sim}{T}_{K_{EP_1}}$ ($i=\overline{1,3}$, $j=\overline{1,5}$)					$\lambda_{2,ij}$ для $\underset{\sim}{T}_{K_{EP_2}}$ ($i=\overline{1,3}$, $j=\overline{1,5}$)					$\lambda_{3,ij}$ для $\underset{\sim}{T}_{K_{EP_3}}$ ($i=\overline{1,3}$, $j=\overline{1,5}$)					$\lambda_{4,ij}$ для $\underset{\sim}{T}_{K_{EP_4}}$ ($i=\overline{1,3}$, $j=\overline{1,5}$)					$\lambda_{5,ij}$ для $\underset{\sim}{T}_{K_{EP_5}}$ ($i=\overline{1,3}$, $j=\overline{1,5}$)				
$\boldsymbol{B}$	0	1	0	0	0	0	0	0	0,89	0,13	0	0	1	0	0	0	0	1	0	0	0	0	0	0,89	0,13
$\boldsymbol{T}$	0	1	0	0	0	0	0	0	0,89	0,13	0	0	1	0	0	0	0,28	0,72	0	0	0	0	0	1	0
$\boldsymbol{E}$	0	1	0	0	0	0	0	0	0,89	0,13	0	0	0,77	0,23	0	0	1	0	0	0	0	0	0	1	0

Пример 3 (2-е состояние)

Согласно 2-го состояния при m = 5 оценочные параметры принимают значения, которые отражены в табл. 8. Произведем классификацию значений $ep_{uz,i}$ по формуле (4) и (5) из [6], результаты которой занесены в табл. 9.

2-е состояние значений оценочных параметров (пример 3) Таблица 8

$\boldsymbol{EP}_i$	$ep_{1,i}$	$ep_{2,i}$	$ep_{3,i}$	$ep_{4,i}$	$ep_{5,i}$
$\boldsymbol{B}$, (i=1)	3,5	10	7,5	7,1	10
$\boldsymbol{T}$, (i=2)	3,2	10	7	6,4	9,7
$\boldsymbol{E}$, (i=3)	3,2	10	8,7	5,1	9,7

Далее, аналогично первому состоянию, вычислим показатель степени риска нарушения ИБ по формуле (6) из [6], т.е. $LRV_{2,1}$ = 32,65, $LRV_{2,2}$ = 90, $LRV_{2,3}$ = 65,47, $LRV_{2,4}$ = 55,4, $LRV_{2,5}$ = 90. Посредством (4) из [6] вычислим $\mu_j(LRV_{2,uz})$, $(uz=\overline{1,5})$, а по выражению (7) из [6] формируются SP_{uz}: $SP_1=$ ($LRV_{2,1}$; $\underset{\sim}{T}_{DR_2}(\mu_2(LRV_{2,1})))$ = (32,65; РН), $SP_2=$ ($LRV_{2,2}$; $\underset{\sim}{T}_{DR_5}(\mu_5(LRV_{2,2})))$ = (90; ПР), $SP_3=$ ($LRV_{2,3}$; $\underset{\sim}{T}_{DR_3}(\mu_3(LRV_{2,3})))$; $\underset{\sim}{T}_{DR_4}(\mu_4(LRV_{2,3})))$ = (65,47; РС(0,11); РВ(0,89)), $SP_4=$ ($LRV_{2,4}$; $\underset{\sim}{T}_{DR_3}(\mu_3(LRV_{2,4})))$ = (55,4; РС), $SP_5=$ ($LRV_{2,5}$; $\underset{\sim}{T}_{DR_5}(\mu_5(LRV_{2,5})))$ = (90; ПР).

Классификация 2-го состояния значений оценочных параметров (пример 3) Таблица 9

EP_i	Значение $\lambda_{uz,ij}$ для $\{\bigcup_{uz=1}^{5} V_{1,uz}\}$, $(uz=\overline{1,5})$																									
	$\lambda_{1,ij}$ для $\tilde{T}_{K_{EP_i1}}$ $(i=\overline{1,3},\ j=\overline{1,5})$					$\lambda_{2,ij}$ для $\tilde{T}_{K_{EP_i2}}$ $(i=\overline{1,3},\ j=\overline{1,5})$					$\lambda_{3,ij}$ для $\tilde{T}_{K_{EP_i3}}$ $(i=\overline{1,3},\ j=\overline{1,5})$					$\lambda_{4,ij}$ для $\tilde{T}_{K_{EP_i4}}$ $(i=\overline{1,3},\ j=\overline{1,5})$					$\lambda_{5,ij}$ для $\tilde{T}_{K_{EP_i5}}$ $(i=\overline{1,3},\ j=\overline{1,5})$				
B	0	0,77	0,22	0	0	0	0	0	0	1	0	0	0,15	0,86	0	0	0	0,46	0,54	0	0	0	0	0	1
T	0	0,94	0,06	0	0	0	0	0	0	1	0	0	0,54	0,47	0	0	0	1	0	0	0	0	0	0	0	1
E	0	0,94	0,06	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	1

На основе выражения (8) из [6], вычислим среднее значение степени риска LR_2 = 66,7 и сформируем для него SP = (66,7; PB).

Графическое представление полученных результатов отображено на рис. 3. и рис. 4.

Как видно из полученных результатов, предлагаемый метод адекватно реагирует на изменения выходных значений оценочных параметров, т.е. при их уменьшении показатели степени риска уменьшаются, а при увеличении – увеличиваются.

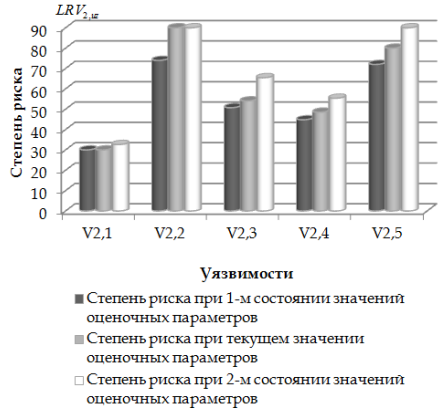

Рис. 3. Результаты вычисления значений для $LRV_{2,uz}$ при разных состояниях: 1-е состояние – уменьшенные значения всех оценочных параметров, относительно текущего состояния; текущие состояние – значения оценочных параметров определенных с помощью базы NVD; 2-е состояние – увеличенные значения всех оценочных параметров, относительно текущего состояния

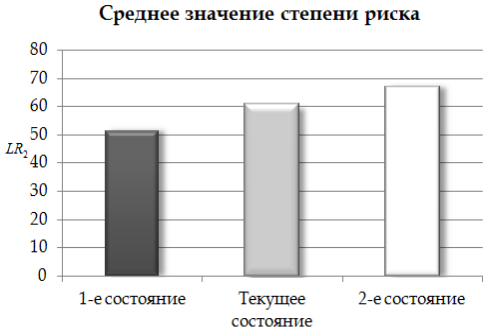

Рис. 4. Результаты вычисления значений для LR_2 при разных состояниях оценочных параметров

Выводы

Таким образом, представленный метод оценивания рисков информационной безопасности на основании открытых баз данных уязвимостей за счет модификации процедур определения множества параметров оценивания риска и оценки текущих значений параметров с возможностью интеграции (в качестве альтернативы оценок экспертов) значений показателей CVSS (версии 3.0), которые представлены в NVD, дает возможность различить уязвимый и атакуемый компоненты, позволяет реализовывать оперативное оценивание и мониторинг (в реальном времени) рисков без привлечения экспертов соответствующей предметной области.

Литература

[1] Банк данных угроз безопасности информации [Электронный ресурс] / Федеральной службой по техническому и экспортному контролю России – М., 2016 – Режим доступа: World Wide Web. – URL: http://bdu.fstec.ru/

[2] Казмирчук С.В. Интегрированный метод анализа и оценивания рисков информационной безопасности / С.В. Казмирчук, А.Ю. Гололобов // Защита информации – 2014. – №3. – С. 252-261.

[3] Корченко А.А. Система формирования нечетких эталонов сетевых параметров / А.А. Корченко // Захист інформації. – 2013. – №3, Т.15. – С. 240- 246.

[4] Корченко А.А. Метод формирования лингвистических эталонов для систем выявления вторжений / А.А. Корченко // Захист інформації. – 2014. – №1. Т.16. – С. 5-12.

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

[6] Корченко А.Г. Качественно-количественный метод оценивания рисков информационной безопасности / А.Г. Корченко, С.В. Казмирчук // Защита информации – 2016. – Том 18 №2, квітень-червень. – С. 157-170.

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

[8] 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 // Защита информации – 2014. – Том 16 №4 (65), жовтень-грудень. – С. 284-291.

[9] Корченко А.Г. Метод преобразования интервалов в нечеткие числа для систем анализа и оценивания рисков / А.Г. Корченко, С.В. Казмирчук // Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине – 2016. – № 1(31). – С. 57-64.

[10] Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А.Г. Корченко – К. : «МК-Пресс», 2006. – 320с.

[11] Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Текст] : НД ТЗІ 3.7-003 – 2005. Чин. 2005.11.08. – К. : ДСТСЗІ СБ України, 2005. – 12 с.

[12] IBM X-Force Exchange [Electronic resource] / IBM Corporation – New York, 2016 – Access mode: World Wide Web. – URL: https:// exchange.xforce.ibmcloud.com/vulnerabilities/109429.

[13] Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013, 34 p.

[14] Common Vulnerability Scoring System v3.0: Specification Document [Electronic resource] / Forum of Incident Response and Security Teams – Morrisville, 2016 – Access mode: World Wide Web. – URL: https://www.first.org/cvss/specification-document.

[15] National Vulnerability Database [Electronic resource] / National Institute of Standards and Technology – Gaithersburg, 2016 – Access mode: World Wide Web. – URL: https:// nvd.nist.gov / home.cfm.

[16] Open Sourced Vulnerability Database [Electronic resource] / Open Security Foundation – Lafayette, 2016 – Access mode: World Wide Web. – URL: https:// http://osvdb.org/.

[17] Vulnerabilities [Electronic resource] / SecurityFocus - Mountain View, 2016 - Access mode: World Wide Web. – URL: http:// www. securityfocus.com /.

[18] Vulnerability Notes Database [Electronic resource] / United States Computer Emergency Readiness Team Murray Lane, 2016 Access mode: World Wide Web. – URL: https:// www. kb.cert.org /vuls/#.

УДК 004.056.5 (045)

Корченко О.Г., Казмірчук С.В. Метод оцінювання ризиків інформаційної безпеки на основі відкритих баз даних уразливостей

Анотація. *В основу побудови різних систем захисту інформації покладено процес оцінювання ризиків. Для його реалізації застосовуються відомі методи аналізу та оцінювання ризиків, засновані на експертних оцінках. Часто в процесі оцінювання доводиться стикатися з ситуаціями, при яких виникають труднощі з залученням експертів або вони не завжди чітко можуть оцінити ту чи іншу вразливість ресурсів інформаційних систем. Також при практичному використанні таких систем виникає необхідність оперативного оцінювання та моніторингу (в реальному часі) ризиків без залучення експертів. У зв'язку з цим доцільно використовувати відповідні бази даних уразливостей. Відомі підходи поки не дозволяють ефективно вирішувати поставлені завдання. Для цього пропонується метод оцінювання ризиків на основі відкритих баз даних уразливостей. Він, на відміну від відомих методів, шляхом використання оцінок, які надаються в існуючих базах даних, дозволяє автоматизувати процес оцінювання ризиків без залучення експертів відповідної предметної області.*

Ключові слова: *ризик, оцінювання ризиків, система оцінювання ризиків, параметри ризику, нечітка змінна, нечіткі числа, перетворення еталонів нечітких чисел, метод оцінювання ризиків, відкриті база даних уразливостей.*

Korchenko O., Kazmirchuk S. The risk assessment method of information security based on open databases vulnerabilities

Abstract. *The basis of information security management system (ISMS) is the processes of analysis and risk assessment. The known methods of analysis and risk assessment based on expert assessments are applied for their implementation. Often in the process of assessment there are situations when the expert cannot always clearly determine a particular vulnerability of Information Systems Resources (ISR). Also at practical use of such systems there is a need for rapid risk assessment and monitoring (real-time) without the involvement of experts. Therefore, it is advisable to use the corresponding database vulnerabilities. The existing approaches do not solve the task effectively. For this purpose, the risk assessment method based on open databases vulnerabilities is offered. It, in contrast to the known methods, through the use of assessments that are available in existing databases, automates the process of risk assessment not involving the experts for this related subject area.*

Key words: *risk, risk assessment, risk assessment system, risk parameters, fuzzy variable, fuzzy numbers, conversion of fuzzy numbers standards, the method of risk assessment, open database vulnerabilities.*

Отримано *16 травня 2016 року*, затверджено редколегією *31 травня 2016 року*