© Korchenko O., Akhmetov B., Kazmirchuk S., Chasnovskiy Ye. Information security risk assessment system – «RISK-CALCULATOR» // Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 2, p. 145-152.

DOI: 10.18372/2225-5036.23.11824

СИСТЕМА ОЦЕНИВАНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – «РИСК-КАЛЬКУЛЯТОР»

Александр Корченко[1], Берик Ахметов[2], Светлана Казмирчук[1], Егор Часновский[1]

[1]Национальный авиационный университет, Украина
[2]Международный казахско-турецкий университет им. Ясави, Республика Казахстан

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 с 2004 года, визит-профессор Университета в Бельско-Бялой (Гуманитарно-техническая академия в Бельско-Бялой, г. Бельско-Бяла, Польша), ведущий научный сотрудник Национальной академии СБ Украины.
Научные интересы: информационная и авиационная безопасность.
Публикации: более 300 научных публикаций, среди которых монографии, словари, энциклопедия, учебники, учебные пособия, научные статьи и патенты на изобретения и др.
E-mail: icaocentre@nau.edu.ua

АХМЕТОВ Берик Бахытжанович, к.т.н.

Год и место рождения: 1985 год, г. Алматы, Казахстан.
Образование: Казахский национальный университет имени аль-Фараби, 2009 г.
Должность: Вице-президент по учебно-методической работе.
Научные интересы: информационная безопасность, бизнес-аналитика, применение ИКТ в образовании.
Публикации: более 40 научных статьей в национальных и международных базах.
E-mail: berik.akhmetov@ayu.edu.kz

КАЗМИРЧУК Светлана Владимировна, к.т.н.

Год и место рождения: 1985 год, г. Алматы, 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, управление информационными рисками.
Публикации: более 90 публикаций, среди которых монографии, учебные пособия, учебно-методические комплексы дисциплин, научные статьи, материалы и тезисы докладов конференций.
E-mail: sv.kazmirchuk@gmail.com

ЧАСНОВСКИЙ Егор Анатольевич

Год и место рождения: 1996 год, с. Ольшаница, Киевская обл., Ракитнянский р-н., Украина.
Образование: Национальный авиационный университет, 2017 год.
Должность: студент кафедры безопасности информационных технологий с 2013 года.
Научные интересы: информационная безопасность, программирование.
Публикации: материалы и тезисы докладов на научных конференциях.
E-mail: egor.chasnovskii@gmail.com

Аннотация. *В обеспечении надежности процессов обработки информации и достижении требуемого уровня информационной безопасности особое место занимает управление рисками нарушения базовых характеристик безопасности ресурсов информационных систем, таких как конфиденциальность, целостность и доступность. На текущий момент для эффективного функционирования большинства существующих систем оценивания рисков информационной безопасности требуется поддержка эксперта. Как следствие, это повышает стоимость и время реализации указанного процесса. Поэтому актуальным является разработка таких систем, которые позволят автоматизировать процесс оценивания рисков информационной безопасности, например, путем использования необходимых для работы входных величин (например, CVSS метрик) из соответствующих баз данных. В связи с этим, предложена структурно-параметрическая модель системы оценивании рисков – «РИСК-КАЛЬКУЛЯТОР», которая, за счет базовых структурных компонент (подсистем формирования первичных и вторичных данных), позволяет минимизировать участие эксперта и максимально автоматизировать процесс формирования необходимых для оценивания параметров. На ее основе разработаны базовый алгоритм и программное средство, которое, в отличие от известных, использует в качестве входных данных оценочные параметры в виде метрик CVSS. Это обеспечивает высокую гибкость и удобство при оценивании рисков безопасностью ресурсов информационных систем в реальном времени без привлечения экспертов соответствующей предметной области.*

Ключевые слова*: риск, оценивание рисков, оценивания рисков информационной безопасности, система оценивания рисков, риск-калькулятор, характеристики риска, безопасность ресурсов информационных систем, CVSS метрики*.

Введение

В обеспечении надежности процессов обработки информации и достижении требуемого уровня информационной безопасности (ИБ) особое место занимает управление рисками нарушения базовых характеристик безопасности ресурсов информационных систем (РИС), таких как конфиденциальность, целостность и доступность [1]. Риски ИБ, возникающие в результате информационной деятельности, можно мониторить посредством их оценивания в процессе функционирования информационной системы (ИС). Это позволит определить корректные, финансово безопасные пути реализации бизнес-процессов на предприятии, в котором функционирует ИС. О важности решения данной задачи свидетельствует, в частности, принятие ряда государственных [2] и международных стандартов в данной области (ISO/IEC 27001 [3], ISO/FDIS 31000 [4] и др.).

Однако, на настоящий момент для большинства существующих систем оценивания рисков (ОР) ИБ требуется поддержка эксперта, что связано с дополнительными финансовыми и временными затратами. Поэтому актуальным является разработка таких систем, которые позволят автоматизировать процесс ОР ИБ, например, путем использования необходимых для работы параметров из соответствующих баз данных (БД), например, CVSS метрик [5]. В связи с этим, цель данной работы направлена на разработку системы ОР ИБ, позволяющей минимизировать участие эксперта и максимально автоматизировать процесс формирования необходимых для оценивания параметров.

Исходя из актуальности, на базе методологии синтеза систем ОР безопасности РИС [6], которая основана на логико-лингвистическом подходе, предложенных методах [1, 7-9], аналитико-синтетической кортежной модели характеристик риска (АСМ) [10], предлагается соответствующая система ОР ИБ, называемая «РИСК-КАЛЬКУЛЯТОР». Такая система, используя CVSS метрики, позволяет осуществлять ОР в режиме реального времени, а также по запросу пользователя трансформировать эталонные лингвистические переменные (ЛП) без привлечения специалистов соответствующей предметной области. Кроме этого, система представляет функцию редактирования указанных метрик, используя встроенный CVSS калькулятор версии 3.0 [5].

Структурно-параметрическая модель предлагаемой системы (рис. 1) состоит из двух базовых компонент, отображающих подсистемы обработки первичных (ППОД) и вторичных данных (ПВОД). Опишем состав каждой из подсистем, построение которых осуществляется согласно известной методологии [6] посредством этапов 3-10.

Подсистема ППОД предназначена для первичной обработки начальных величин и включает в себя модуль инициализации входных данных (МИД), а также модули формирования (МФЭ) и преобразования (МПЭ) эталонных значений.

Подсистема ПВОД, используя CVSS метрики, осуществляет преобразование первичных параметров, поступающих с ППОД с целью формирования окончательных оценок степени риска (СР). Она состоит из модуля взвешивания оценочных параметров (МВП) и их корректировки (МКП), а также модулей оценки СР (МСР) и генерации отчета (МГО).

Рассмотрим функциональное назначение каждого из модулей подсистем. Так, МИД (в соответствии с этапами 3 и 4 методологии [6]) предназначен для формирования и идентификации множества РИС и уязвимостей объекта оценивания. Здесь на основе множества $\boldsymbol{RIS}$ [8] для указанного объекта экспертами определяется требуемое множество РИС (и соответственно их идентификаторов) $\boldsymbol{RISO} = \{\bigcup_{rs=1}^{ro} \boldsymbol{RISO}_{rs}\}$, $(rs = \overline{1, ro})$, где ro – количество оцениваемых РИС на объекте. Далее относительно всех $\boldsymbol{RISO}_{rs}$ определяются множества их уязвимостей $\{\bigcup_{rs=1}^{ro} \boldsymbol{V}_{rs}\} = \{\bigcup_{rs=1}^{ro}\{\bigcup_{uz=1}^{n_{rs}} V_{rs,uz}\}\}$, $(rs = \overline{1, ro}, \quad uz = \overline{1, n_{rs}})$, где n_{rs} – возможное количество идентифицированных уязвимостей rs-того оцениваемого РИС

($\boldsymbol{RISO}_{rs}$). В качестве входных данных для МИД могут использоваться, например, результаты работы программы для проверки системы на проникновение (Penetration test). Такое программное обеспечение, как правило, выполняет анализ указанного объекта, производя поиск уязвимостей его РИС в киберпространстве (согласно ISO/IEC 27032:2012 под киберпространством можем понимать сложную сущность, которая реально существует в виде глобальной совокупности процессов взаимодействия людей, программного обеспечения и сервисов Интернет в сетях (включая подключенное к ним технологическое оборудования), но которая при этом никак не проявляется в какой-либо известной, материальной форме).

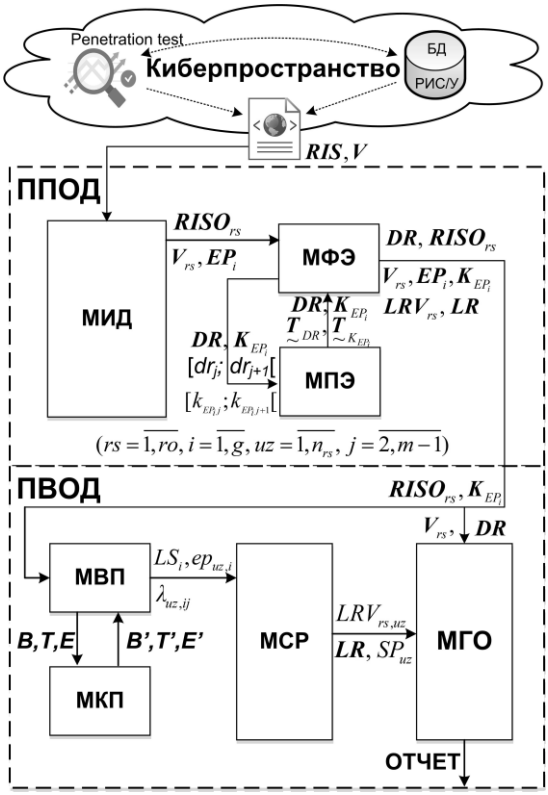

Рис. 1. Структурно-параметрическая модель системы ОР ИБ – «РИСК-КАЛЬКУЛЯТОР»

Таким образом, формируется список в виде множества уязвимостей РИС исследуемого объекта. Для получения множества РИС и множества соответствующих уязвимостей в МИД выполняется обработка полученного из специализированного программного обеспечения (уровня – Penetration test), соответствующего отчета, который содержит в себе информацию об РИС и уязвимостях с указанными CVSS метриками. Далее, осуществляется инициализация списка уязвимостей и РИС, для последующей передачи в МФЭ. В результате работы МИД на вход МФЭ поступают все идентифицированные $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$ и их CVSS метрики.

Далее в МФЭ (согласно этапа 5 методологии [6]) осуществляется формирование множества параметров:

– $\boldsymbol{LR} = \{\bigcup_{rs=1}^{ro} \boldsymbol{LR}_{rs}\}$ $(rs = \overline{1,ro})$, где $\boldsymbol{LR}_{rs}$ – количественная оценка риска rs– того РИС на объекте (используется для $\boldsymbol{RISO}_{rs}$);

– $\boldsymbol{LRV} = \{\bigcup_{rs=1}^{ro} \boldsymbol{LRV}_{rs}\} = \{\bigcup_{rs=1}^{ro} \{\bigcup_{uz=1}^{n_{rs}} LRV_{rs,uz}\}\}$ $(rs = \overline{1,ro}, uz = \overline{1,n_{rs}})$, где $LRV_{rs,uz}$ – количественная оценка риска по каждой uz– той уязвимости rs– того РИС на объекте (используется для ОР по каждой уязвимости, отображенной идентификатором $V_{rs,uz}$);

– $\boldsymbol{DR}$, где ЛП «СТЕПЕНЬ РИСКА», представляется в виде кортежа [1, 7-9] <$\boldsymbol{DR}$, $\underset{\sim}{T}_{DR}$, $\boldsymbol{X}_{DR}$> с базовыми терм-множествами, определяемыми m-термами $\underset{\sim}{\boldsymbol{T}}_{DR} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{DR_j}$ (используется для отображения результата ОР);

– $\boldsymbol{EP} = \{\bigcup_{i=1}^{g} \boldsymbol{EP}_i\}$ $(i = \overline{1,g})$, где g – количество множеств оценочных параметров (используется для обеспечения процесса оценивания, за основу берутся показатели CVSS);

– $\boldsymbol{K}_{EP_i}$, где ЛП «УРОВЕНЬ ОЦЕНОЧНОГО ПАРАМЕТРА $\boldsymbol{EP}_i$» определяется кортежем [1, 7-9] < $\boldsymbol{K}_{EP_i}$, $\underset{\sim}{T}_{K_{EP_i}}$, $\boldsymbol{X}_{EP_i}$ > с базовыми терм-множествами, определяемыми m-термами $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{K_{EP_ij}}$ (используется для отображения результатов оценивания с использование метрик CVSS).

Сформированные ЛП $\boldsymbol{DR}$ и $\boldsymbol{K}_{EP_i}$ передаются на вход МПЭ, где (согласно этапам 6-8 методологии [6]) для каждого из термов $\underset{\sim}{T}_{DR_1}$,…, $\underset{\sim}{T}_{DR_j}$,…, $\underset{\sim}{T}_{DR_m}$ и $\underset{\sim}{T}_{K_{EP_i1}}$, $\underset{\sim}{T}_{K_{EP_i2}}$,…, $\underset{\sim}{T}_{K_{EP_ij-1}}$, $\underset{\sim}{T}_{K_{EP_ij}}$, …, $\underset{\sim}{T}_{K_{EP_im}}$ реализуется преобразование [11] соответственно заданного интервала значений $[dr_1; dr_2[, \ldots, [dr_j; dr_{j+1}[, \ldots, [dr_m; dr_{m+1}]$ и $[k_{EP_i1}; k_{EP_i2}[, [k_{EP_i2}; k_{EP_i3}[, \ldots, [k_{EP_ij-1}; k_{EP_ij}[, [k_{EP_ij}; k_{EP_ij+1}[, \ldots, [k_{EP_im}; k_{EP_im+1}]$ в НЧ. Также в МПЭ реализована процедура варьирования порядком ЛП. Так, для эквивалентного преобразования m-мерных термов НЧ ЛП $\boldsymbol{DR}^{(m)}$ в $\boldsymbol{DR}^{(m-n)}$ или $\boldsymbol{DR}^{(m+n)}$ и $\boldsymbol{K}_{EP_i}^{(m)}$ в $\boldsymbol{K}_{EP_i}^{(m-n)}$ или $\boldsymbol{K}_{EP_i}^{(m+n)}$ в МПЭ используются методы трансформирования эталонов ЛП [12, 13]. В результате преобразований на выход ППОД поступают $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$ и их CVSS метрики, $\boldsymbol{EP}_i$, ЛП $\boldsymbol{DR}$ и $\boldsymbol{K}_{EP_i}$, а также сформированные множества $\boldsymbol{LR}$ и $\boldsymbol{LRV}_{rs}$ для ОР.

В МВП ПВОД (формируется согласно этапа 9 методологии [6]) определяются уровни значимости оценочных параметров LS_i $(i = \overline{1,g})$ и их текущих

значений $\boldsymbol{ep}_{uz,i}$ из ППОД, например, $\{\bigcup_{i=1}^{3} \boldsymbol{EP}_i\} = \{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_3\} = \{\boldsymbol{B}, \boldsymbol{T}, \boldsymbol{E}\}$ $(i = \overline{1,3})$ [8, 9]. Далее посредством эталонных значений осуществляется процесс фаззификации, который связан с определением принадлежности $\boldsymbol{ep}_{uz,i}$ заданному НЧ, по которому с помощью выражения (5) в [8] формируются значения $\lambda_{uz,ij}$. Также в МВП осуществляется графическая интерпретация оценочных параметров $\boldsymbol{B}$, $\boldsymbol{T}$ и $\boldsymbol{E}$ (см. рис. 2).

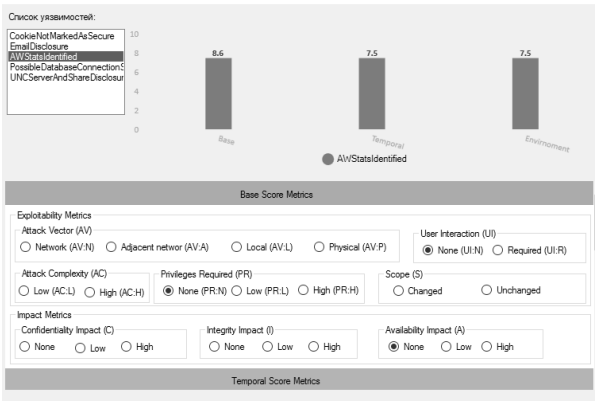

Рис. 2. Встроенный CVSS-калькулятор с графической интерпретацией CVSS метрик

В случае необходимости возможна корректировка CVSS метрик с помощью МКП, в котором реализуется их переопределение за счет встроенного CVSS-калькулятора (см. рис. 2). Скорректированные параметры $\boldsymbol{B}'$, $\boldsymbol{T}'$ и $\boldsymbol{E}'$ передаются обратно в МВП.

Данные из МВП LS_i, $\boldsymbol{ep}_{uz,i}$ и $\lambda_{uz,ij}$ поступают в МСР, где на основе этапа 10 методологии [6], для каждой уязвимости, отображенной идентификатором $V_{rs,uz}$ реализуется оценивание СР $LRV_{rs,uz}$, а также вычисляется среднее значение $\boldsymbol{LR}_{rs}$ для РИС. Далее, на основании вычисленного значения $LRV_{rs,uz}$, $\boldsymbol{LR}_{rs}$ и построенных эталонов в ППОД, осуществляется процесс дефаззификации, который связан с формированием структурированного параметра СР SP_{uz}, позволяющего получить числовые значения СР и его лингвистическую интерпретацию.

На основании МГО, с учетом результатов работы ППОД и ПВОД, генерируется отчет по оценкам СР (см. рис. 3), который содержит $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$, $LRV_{rs,uz}$, $\boldsymbol{LR}_{rs}$, их лингвистические эквиваленты и графическую интерпретацию результатов.

Предложенная система ОР ИБ – «РИСК-КАЛЬКУЛЯТОР», например, может быть реализована программно и работать на основе предложенного базового алгоритма (рис. 4).

Согласно этому алгоритму, работа системы начинается с инициализации списка уязвимостей и CVSS оценок (вершина 1) посредством специализированной программы проверки системы на проникновение (Penetration test). Данная процедура в программной реализации может, например, выполнятся за счет функции OpenXMLFile(), которая открывает файл в формате XML и реализует его парсинг. Парсинг XML файла используется для того, чтобы осуществить инициализацию (наполнение) полей класса Vulnerability со следующей структурой:

```
class Vulnerability
  {
    public string Id { get; set; }
    public string Description { get; set; }
    public string VulClass { get; set; }
    public string vectorCVSS { get; set; }
    public Metrics metrics;
    public Vulnerability()
    {
      metrics = new Metrics();
    }}.
```

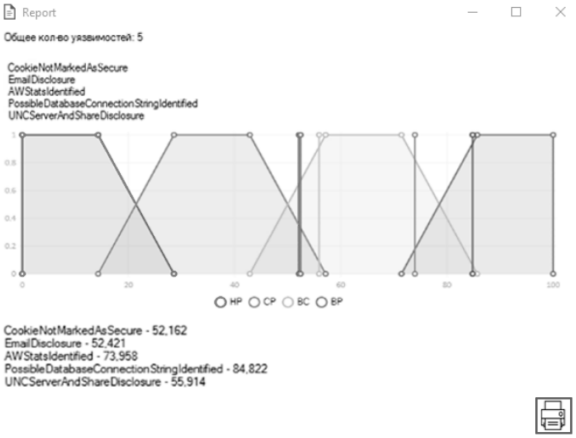

Рис. 3. Пример сгенерированного отчета

После идентификации очередной уязвимости (класс Vulnerability) ее характеристики помещаются в контейнер List, в результате чего образовывается структура – List <Vulnerability>. Далее, после генерации списка уязвимостей (вершина 2) его содержимое записывается в компонент ListBox с $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$ и их CVSS оценки.

Далее в цикле (вершина 3) осуществляется выбор уязвимостей (вершина 4) с ListBox (Select Vul) и их графическая интерпретация (вершина 5) CVSS метрик (рис. 2). Этот процесс обеспечивает соответствующий обработчик события – функция lbVul CVSS_ SelectedIndexChanged. В момент, когда происходит изменение индекса выделенного элемента компонента ListBox возникает событие SelectedIndexChanged. Функция lbVulCVSS_SelectedIndexChanged выполняет графическое отображение CVSS метрик на основе библиотеки LiveChart. Отображение CVSS метрик осуществляется в виде столбчатой диаграммы (см. рис. 2), что достигается посредством следующего блока программного листинга:

```
chartCVSS.Series.Add(new ColumnSeries()
        {
          Title = vulList[lb.SelectedIndex].Description,
          Values = new Chart-
Values<ObservableValue>()
          {
            new ObservableVal-
ue(vulList[lb.SelectedIndex].metrics.baseVector.Commo
nScore),
            new ObservableVal-
ue(vulList[lb.SelectedIndex].metrics.tempVector.Comm
onScore),
```

new ObservableVal-
ue(vulList[lb.SelectedIndex].metrics.envirVector.CommonScore)

},
DataLabels = true});

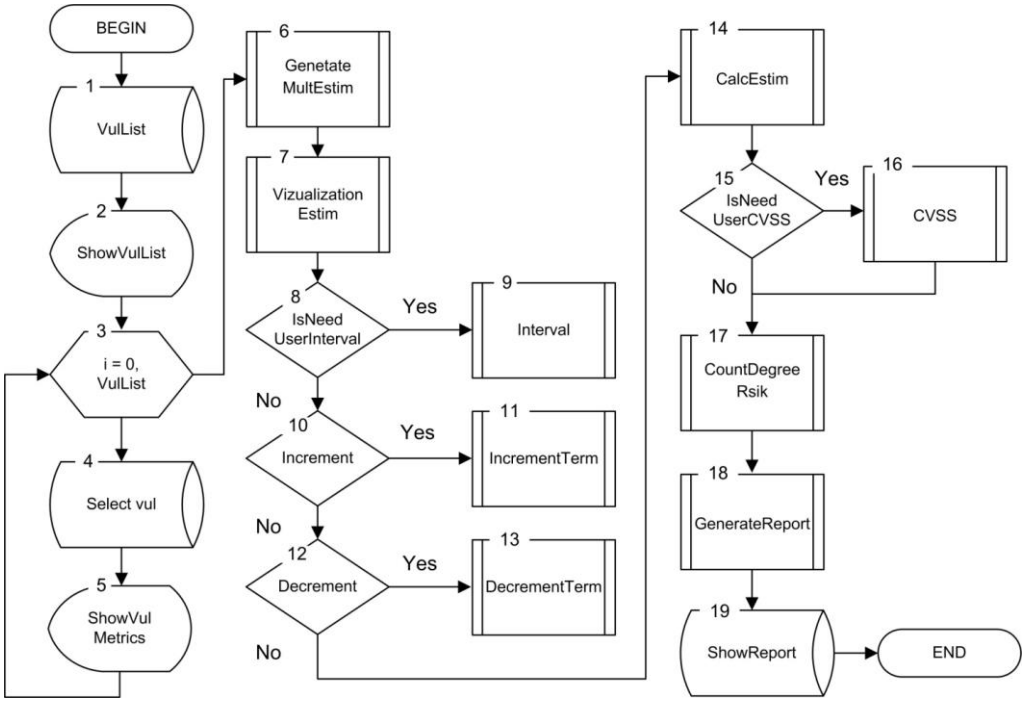

Рис. 4. Базовый алгоритм работы системы оценивания рисков ИБ

Далее, посредством предопределенного процесса (вершина 6) осуществляется формирование ЛП $\boldsymbol{K}_{EP_i}$ и $\boldsymbol{DR}$, а также инициализируются множества для последующих оценок $\boldsymbol{LR}$ и $\boldsymbol{LRV}_{rs}$.

После формирования необходимых лингвистических термов выполняется преобразование заданных интервалов в НЧ, образующих лингвистические эталоны и реализуется их графическая интерпретация (вершина 7). Для наглядности, полученные CVSS метрики по каждой уязвимости, выводятся на графике с эталонными значениями $\boldsymbol{EP}_i$ (см. рис. 5). Представление термов ЛП $\boldsymbol{K}_{EP_i}$ в графическом виде (в соответствие с программной реализацией системы) обеспечивается структурой TrapezeCreator, которая может иметь, например, следующие поля:

```
struct Trapeze
  {
    public string degreeRisk;
    public double a { get; set; }
    public double b11 { get; set; }
    public double b21 { get; set; }
    public double c { get; set; }
  }.
```

Интервалы, которые будут использованы для преобразования в НЧ описываются структурой Interval, состоящей из следующих полей:

```
struct Interval
  {
    public double a { get; set; }
    public double b { get; set; }
  }.
```

Графическая интерпретация полученных результатов (согласно предложенной программной реализации) осуществляется с помощью функции List <Trapeze> CreateTrapezeList (double lengthAsixX, int countTrap, params double [] intervalArr). Далее, с помощью подпрограмм Interval, IncrementTerm, DecrementTerm и условных вершин (вершины 8-13), используемых для контроля необходимости в дополнительной обработке данных, т.е. преобразовании заданных интервалов в НЧ, реализации процесса декрементирования и инкрементирования порядка ЛП.

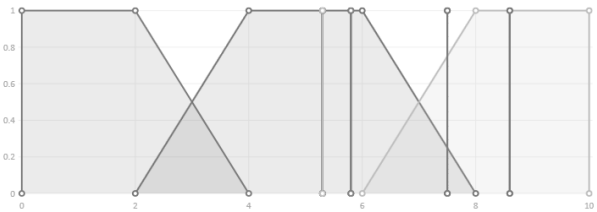

Рис. 5. Графическая интерпретация полученных CVSS метрик и эталоны оценочных параметров

Инициализация нового интервала в программе осуществляется посредством следующего блока программного листинга (вершины 8-9):

```
double[] interval = new double [intervalList.
Count * 2];
for (int i = 0, k = 0; i < interval.Length; i++, k++)
      {
        interval[i] = intervalList[k].a;
        interval[++i] = intervalList[k].b;}.
```

Интервалы образуются из предварительно сформированного списка intervalList, что имеет тип List <Interval> и заполняются посредством следующего блока программного листинга:

```
private void bSetInterval_Click(object sender,
EventArgs e)
    {
```

```
string[] arrInterval = interval.Split(':');
double a = Convert.ToDouble(arrInterval[0]);
double b = Convert.ToDouble(arrInterval[1]);
intervalList.Add(new Interval() { a = a, b = b });}.
```

Процедура инкрементирования (вершины 10-11) или декрементирования (вершины 12-13) может осуществляться, например, с помощью разработанных функций List <Trapeze> IncrementTrapezeList (List <Trapeze> trapList, double lengthAsixX) или List <Trapeze> DecrementTrapezeList (List <Trapeze> trapList, double lengthAsixX).

На основании полученных CVSS метрик реализуется (вершина 14) оценка LS_i и классификация $\lambda_{uz,ij}$ полученных $\boldsymbol{ep}_{uz,i}$ (фаззификация). При необходимости (вершина 15), осуществляется корректировка CVSS метрик ***B***, ***T*** и ***E*** (вершина 16).

Далее, с помощью выражения (6) в [8] и полученных данных LS_i и $\lambda_{uz,ij}$, осуществляется оценивание СР $LRV_{rs,uz}$ (вершина 17) для каждой уязвимости, отображенной идентификатором $V_{rs,uz}$, а также вычисляется среднее значение $\boldsymbol{LR}_{rs}$. Здесь, на основании полученных $LRV_{rs,uz}$, $\boldsymbol{LR}_{rs}$ и построенных эталонов в ППОД, формируется структурированный параметр СР SP_{uz} (дефаззификация).

В результате проведенных расчетов по качественно-количественному методу ОР ИБ [8] (вершина 18) формируется отчет по оценкам СР (рис. 4), который содержит $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$, $LRV_{rs,uz}$, $\boldsymbol{LR}_{rs}$, их лингвистические эквиваленты, а также осуществляется графическая интерпретация (вершина 19) результатов (рис. 3).

Для верификации работы разработанного программного обеспечения (см. рис. 6), было произведено соответствующее экспериментальное исследование. Здесь, для тестирования объекта оценивания на проникновение использовано программное средство проверки системы на уязвимости – «Netsparker» (рис. 7). В результате сканирования был сформирован XML-файл со списком РИС и их уязвимостей (рис. 8) для дальнейшего использования в качестве входных данных разработанной системы ОР ИБ.

Далее осуществляется инициализация входных данных в виде списка уязвимостей в ListBox. На рис. 9 и рис. 10 соответственно визуализированы примеры реализации функции трансформирования порядка ЛП ***DR***, которая выполняется по запросу пользователя посредством активизации процесса инкрементирования и декрементирования.

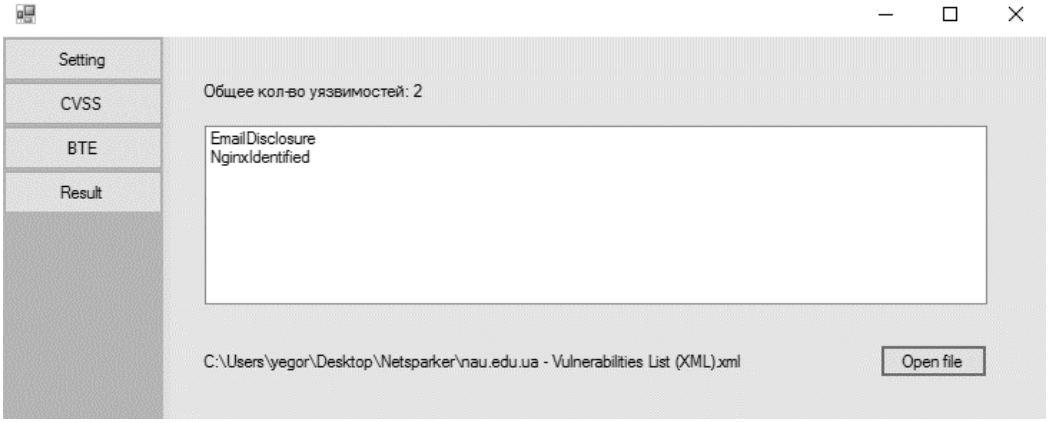

Рис. 6. Фрагмент интерфейса программной системы – «РИСК-КАЛЬКУЛЯТОР»

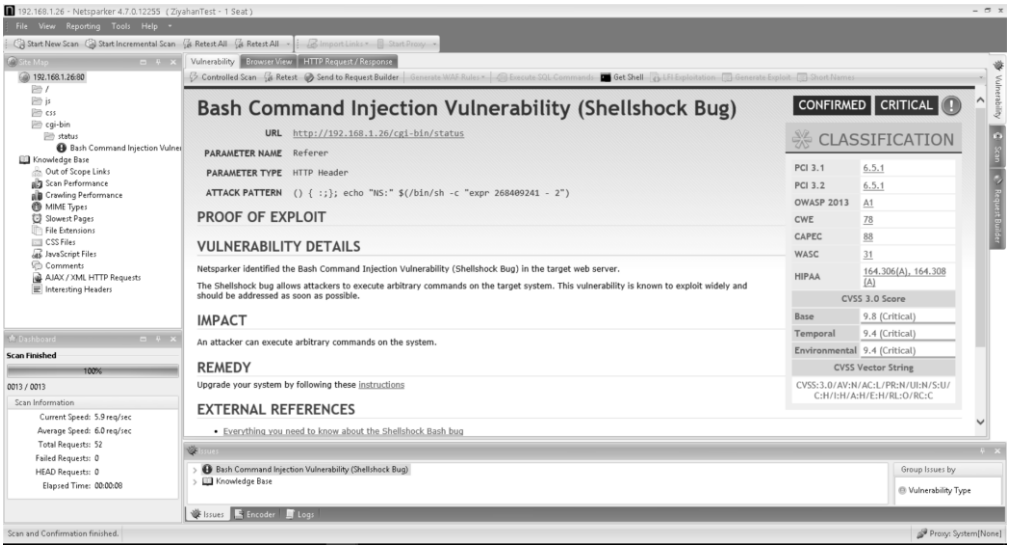

Рис. 7. Интерфейсная часть программы проверки на уязвимости «Netsparker»

Рис. 8. XML файл со списком уязвимостей

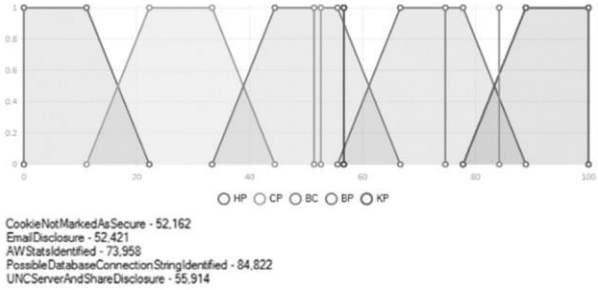

Рис. 9. Результат инкрементирования порядка ЛП ***DR***

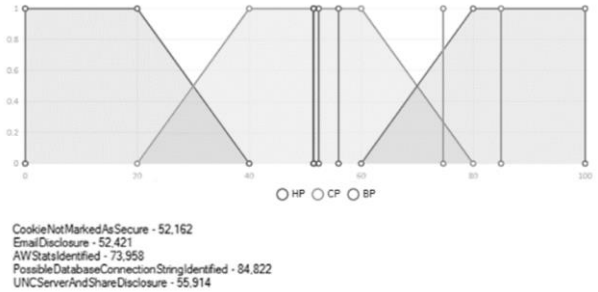

Рис. 10. Результат декрементирования ЛП ***DR***

На основании полученной информации об оценочных компонентах и уязвимостях система производит вычисление (вершина 17) СР для каждой уязвимости и с помощью подпрограммы (вершина 18), реализующей функции МГО, осуществляет графическую интерпретацию принадлежности уязвимости соответственному терму ЛП ***DR*** при m=4 (рис. 11). Все полученные результаты фиксируются в отчете, генерируемым МГО.

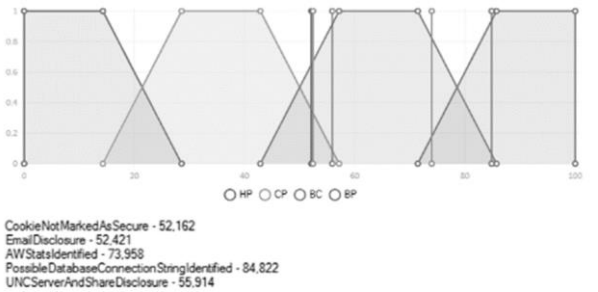

Рис. 11. Результат вычисления СР для идентифицированных уязвимостей на объекте оценивания

Вывод

Таким образом, впервые была разработана структурно-параметрическая модель системы ОР ИБ – «РИСК-КАЛЬКУЛЯТОР», которая, за счет структурных компонент подсистем, формирования первичных и вторичных данных, а также составляющих их модулей инициализации входных данных, формирования и преобразования эталонных значений, взвешивания оценочных параметров и их корректировки, оценивания СР и генерации отчета, в которых реализованы предложенные методы (качественно-количественный [8], оценивания на основе баз данных уязвимостей [9], инкрементирования и декрементирования порядка лингвистических переменных [12, 13]), позволяет обеспечить высокую гибкость и удобство при оценивания рисков безопасностью РИС без участия экспертов соответствующей предметной области.

Также на основе предложенной структурно-параметрической модели разработаны базовый алгоритм и соответствующее программное средство оценивания в виде прикладной программной системы – «РИСК-КАЛЬКУЛЯТОР», которая (в отличие от известных [7]), использует значение CVSS (версий 2.0 и 3.0) показателей, представленных в соответствующих базах данных и позволяет реализовывать оценивание рисков безопасности РИС в реальном времени.

Литература

[1] А. Корченко, Построение систем защиты информации на нечетких множествах. Теория и практические решения, К.: МК-Пресс, 2006, с.320.

[2] «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, с. 12.

[3] «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, p. 34.

[4] «International standard Risk management. Principles and guidelines», ISO/FDIS 31000:2009(E), International Organization for Standardization, JISC, 2009, p. 24.

[5] «Common Vulnerability Scoring System v3.0: User Guide» [Electronic resource], Forum of Incident Response and Security Teams, Morrisville, 2016, [Online]. Access mode: http://www.first.org/cvss/us er-guide.

[6] С. Казмирчук, А. Гололобов, А. Арджомандифард, «Синтез систем оценивания рисков безопасности ресурсов информационных систем», *Вісник Інженерної академії наук*, №3, с. 78-81. 2016.

[7] А. Корченко, А. Архипов, С. Казмирчук, Анализ и оценивание рисков информационной безопасности. Монография, Киев: ООО «Лазурит-Полиграф», 2013, с. 275.

[8] А. Корченко, С. Казмирчук, «Качественно-количественный метод оценивания рисков информационной безопасности», *Захист інформації*, №2, с. 157-170, 2016.

[9] А. Корченко, С. Казмирчук, «Метод оценивания рисков информационной безопасности на основе открытых баз данных уязвимостей», *Безпека інформації*, №2, с. 216-226, 2016.

[10] А. Корченко, С. Казмирчук, Ю. Дрейс, А. Гололобов, «Бистабильная интегрированная кортежная модель характеристик риска», *Защита информации*, №4, с. 314-323, 2016.

[11] А. Корченко, С. Казмирчук, «Метод преобразования интервалов в нечеткие числа для систем анализа и оценивания рисков», *Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине*, № 1(31), с. 57-64, 2016.

[12] А. Корченко, Б. Ахметов, С. Казмирчук, Н. Сейлова, А. Гололобов, «Метод n-кратного понижения числа термов лингвистических переменных в задачах анализа и оценивания рисков», *Захист інформації*, Т. 16, №. 4, с. 284-291, 2014.

[13] А. Корченко, Б. Ахметов, С. Казмирчук, М. Жекамбаева, «Метод n-кратного инкрементирования числа термов лингвистических переменных в задачах анализа и оценивания рисков», *Безпека інформації*, Т.21, №2, с. 191-200, 2015.

УДК 004.056.5 (045)

Корченко О.Г., Ахметов Б.Б., Казмірчук С.В., Часновський Є.А. Система оцінювання ризиків інформаційної безпеки - «РИЗИК-КАЛЬКУЛЯТОР»

Анотація. *В забезпеченні надійності процесів обробки інформації та досягненні необхідного рівня інформаційної безпеки особливе місце займає управління ризиками порушення базових характеристик безпеки ресурсів інформаційних систем, таких як конфіденційність, цілісність та доступність. На поточний момент для ефективного функціонування більшості існуючих систем оцінювання ризиків інформаційної безпеки потрібна підтримка експерта. Як наслідок, це підвищує вартість і час реалізації зазначеного процесу. Тому актуальною є розробка таких систем, які дозволять автоматизувати процес оцінювання ризиків інформаційної безпеки, наприклад, шляхом використання необхідних для роботи вхідних величин (наприклад, CVSS метрик) з відповідних баз даних. У зв'язку з цим запропоновано структурно-параметричну модель системи оцінюванні ризиків - «РИЗИК-КАЛЬКУЛЯТОР», яка за рахунок базових структурних компонент (підсистем формування первинних і вторинних даних) дозволяє мінімізувати участь експерта і максимально автоматизувати процес формування необхідних для оцінювання параметрів. На її основі розроблені базовий алгоритм і програмний засіб, який, на відміну від відомих, використовує в якості вхідних даних оціночні параметри у вигляді метрик CVSS. Це забезпечує високу гнучкість і зручність при оцінюванні ризиків безпекою ресурсів інформаційних систем в реальному часі без залучення експертів відповідної предметної області.*

Ключові слова: *ризик, оцінювання ризиків, оцінювання ризиків інформаційної безпеки, система оцінювання ризиків, ризик-калькулятор, характеристики ризику, безпека ресурсів інформаційних систем, CVSS метрики.*

Korchenko O., Akhmetov B., Kazmirchuk S., Chasnovskiy Ye. Information security risk assessment system – «RISK-CALCULATOR»

Abstract. *In order to ensure the reliability of information processing procedures and to achieve the required level of information security, risk management of basic characteristics violations of information security system resources has a special place, such as confidentiality, integrity and accessibility. At the moment, to ensure that most existing systems of information security risks assessment function effectively, an expert support is required. As a result, it increases the cost and time of realization of the specified process. Therefore, it is relevant to develop such systems that will allow to automate the process of information security risks assessment, for example, by using the input values necessary for the operation (for example, CVSS metrics) from the relevant databases. In this regard, the structural-parametric model of the risk assessment system is proposed – "RISK-CALCULATOR", which, due to the basic structural components (subsystems of primary and secondary data formation), allows to minimize the expert's participation and maximizes the process of formation of the parameters necessary for the assessment. Based on this, a basic algorithm and a software tool have been developed, which, unlike the known ones, uses as input the estimated parameters as CVSS metrics. This provides high flexibility and convenience when assessing the risks of information security systems resources in real time without involving experts in the relevant subject area.*

Key words: *risk, risk assessment, information security risk assessment, risk assessment system, risk calculator, risk characteristics, information security systems resources, CVSS metrics.*

Отримано 21 *червня 2017 року*, затверджено редколегією 28 *липня 2017 року*