Real-time Cybersecurity Risk Assessment

Oleksandr Korchenko [1], Svitlana Kazmirchuk [1], Tetiana Panivko-Babenko [1], Stanislav Milevskyi [2] and Volodymyr Aleksiyev [2]

[1] *National Aviation University, Liubomyra Huzara ave., Kyiv, 03058, Ukraine*
[2] *Simon Kuznets Kharkiv National University of Economics, Nauki ave., 9a, Kharkiv, 61166, Ukraine*

Abstract

The structural solution of the real-time information security risks assessment system is developed, which, due to the structural components of the subsystems of primary and secondary data generation, as well as their components of input data initialization modules, formation and conversion of reference values, weighing evaluation parameters and their adjustment, evaluation of risk degree and report generation, in which the proposed method is implemented, allows to provide certain properties of adaptability and efficiency in risks assessment in real time.

Keywords

Information security, risks assessment, risk degree, software, report

1. Introduction

Often in the risks analysis and assessment (RAA) it is not always possible to involve relevant specialists, and there are situations in which the expert can not always unambiguously assess a particular vulnerability of information systems resources (ISR). It is proposed to use appropriate databases (DB) of vulnerabilities (in which their quantitative estimates are presented), such as the National Vulnerability Database (NVD), Open Sourced Vulnerability Database (OSVDB), IBM X-Force, US-CERT VND, SecurityFocus and etc. The basic component of such databases is CVSS - indicators that can be used as an alternative to expert estimates.

In practice, for example, there may be situations where it is necessary to carry out operational assessment and monitoring (real-time) of risks without the involvement of these experts, and the available methods and tools of RA do not provide such an opportunity.

On this basis, we will develop a method of risk assessment (RA), which will implement an alternative RA using known databases without the involvement of experts in the relevant field.

Use only styles embedded in the document. For paragraph, use Normal. Paragraph text. Paragraph text. Paragraph text. Paragraph text.

2. Method of assessing information security risks based on open databases of vulnerabilities

Let's consider in details its work, which is based on 11 steps.

Step 1 (Determining the complete set of RIS identifiers and vulnerabilities)

The first step determines the complete set of identifiers of all RIS, ie

$$\boldsymbol{RIS} = \{\bigcup_{rs=1}^{r} RIS_{rs}\} \quad (rs = \overline{1,r}),$$

where r – the number of all resources (and, accordingly, their identifiers), as well as the full set of vulnerabilities

$$\boldsymbol{V} = \{\bigcup_{uz=1}^{n} V_{uz}\} \quad (uz = \overline{1,n}),$$

where n – the number of all vulnerabilities (and, accordingly, their identifiers). Based on and experts can identify sets of RIS and vulnerabilities

EMAIL: oleksandr.korchenko@npp.nau.edu.ua (A. 1); sv.kazmirchuk@nau.edu.ua (A. 2); pani.tasha@gmail.com (A. 3); Stanislav.Milevskiy@hneu.net (A. 4); aleksiyev@gmail.com (A. 5)
ORCID: 0000-0003-3376-0631 (A. 1); 0000-0001-6083-251X (A. 2); 0000-0003-2085-3783 (A. 3); 0000-0001-5087-7036 (A. 4); 0000-0001-6767-7524 (A. 4)

by object of assessment. To create appropriate sets (as a basis), for example, a known database of NVD vulnerabilities can be used.

Step 2 (Determining the set of RIS identifiers and vulnerabilities for the object of evaluation)

Here, based on the set $\boldsymbol{RIS}$ for a specific object of evaluation, experts determine the required set of RIS (and, accordingly, their identifiers) $\boldsymbol{RISO}$ ($\boldsymbol{RISO} \subset \boldsymbol{RIS}$), that is

$$\boldsymbol{RISO} = \{\bigcup_{rs=1}^{ro} RISO_{rs}\} \ (rs = \overline{1, ro}),$$

where ro – the number of assessed RIS at the facility. Next for every $RISO_{rs}$ the sets of their vulnerabilities are determined $\boldsymbol{V}_{rs} \subset \boldsymbol{V}$ (and, accordingly, their identifiers), ie

$$\{\bigcup_{rs=1}^{ro} \boldsymbol{V}_{rs}\} = \{\bigcup_{rs=1}^{ro} \{\bigcup_{uz=1}^{n_{rs}} V_{rs,uz}\}\} \ (rs = \overline{1, ro}, \ uz = \overline{1, n_{rs}}),$$

where n_{rs} – possible number of identified vulnerabilities rs- of the estimated RIS $(RISO_{rs})$.

Step 3 (Determining the set of risk assessment parameters)

Here we introduce a set of risk assessments $\boldsymbol{LR}$ for the defined in the second step $\boldsymbol{RISO}$, ie at $rs = \overline{1, ro}$

$$\exists \boldsymbol{LR} = \{\bigcup_{rs=1}^{ro} LR_{rs}\} = \{LR_1, ..., \ LR_{rs}\}.$$

So, for RE for each vulnerability reflected by the identifier $V_{rs,uz}$ introduce sets $\boldsymbol{LRV}_{rs}$ at $rs = \overline{1, ro}$ and $uz = \overline{1, n_{rs}}$, ie

$$\exists \{\bigcup_{rs=1}^{ro} \boldsymbol{LRV}_{rs}\} = \{\bigcup_{rs=1}^{ro} \{\bigcup_{uz=1}^{n_{rs}} LRV_{rs,uz}\}\},$$

where $LRV_{rs,uz}$ – quantitative risk assessment for each *uz*-th vulnerability of *rs*-th PIC on yhe object. To display the result of the RA, we will use the LV "RISK DEGREE" (***RD***), presented in the form of a tuple.

Further, to ensure the evaluation process, indicators are taken as a basis CVSS [1] with NVD. To do this, define the required sets of parameters $\boldsymbol{EP}_i$, $(i = \overline{1, g})$, used for evaluation, ie $\boldsymbol{EP} = \{\bigcup_{i=1}^{g} \boldsymbol{EP}_i\} = \{EP_1, EP_2, ..., \ EP_g\}$, where g – the number of sets of such parameters.

Note that for version 3 estimations of CVSS [1], in which, unlike version 2.0, the metrics of operation (***AC, AV, PR, UI***) calculated for the vulnerable component, and impact metrics (***C, I, A***) for the attacker. This makes it possible to distinguish between vulnerable and attacking components, for example, when g = 3 can be determined by the following sets of values –

$$\{\bigcup_{i=1}^{3} \boldsymbol{EP}_i\} = \{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_3\} = \{\boldsymbol{B}, \ \boldsymbol{T}, \ \boldsymbol{E}\}$$

$$(i = \overline{1,3}),$$

where:

$\boldsymbol{B}$ – **basic (Base) estimations**, which are presented as a set

$$\boldsymbol{B} = \{\bigcup_{uz=1}^{n_{rs}} B_{uz}\} \ (uz = \overline{1, n_{rs}}),$$

whose members are formed on the basis of a group of sets of parameters $\boldsymbol{AV}_{uz}$, $\boldsymbol{AC}_{uz}$, $\boldsymbol{PR}_{uz}$, $\boldsymbol{S}_{uz}$, $\boldsymbol{UI}_{uz}$, $\boldsymbol{C}_{uz}$, $\boldsymbol{I}_{uz}$, $\boldsymbol{A}_{uz}$ $(uz = \overline{1, n_{rs}})$, where:

$\boldsymbol{AV}_{uz}$ – cyber-attack vector, which is represented as a set

$$\boldsymbol{AV}_{uz} = \{\bigcup_{av=1}^{4} AV_{uz,av}\}$$

$$= \{AV_{uz,1}, ..., AV_{uz,4}\} = \{N, A, L, P\}$$

$(uz = \overline{1, n_{rs}}, av = \overline{1,4})$, where: N – «Network» = 0,85; *A* – «Connected network» = 0,62; *L* – «Local access» = 0,55; *P* – «Physical access» = 0,2,

$\boldsymbol{AC}_{uz}$ – the complexity of the cyber-attack, represented by the set

$$\boldsymbol{AC}_{uz} = \{\bigcup_{ac=1}^{2} AC_{uz,ac}\}$$

$$= \{AC_{uz,1}, AC_{uz,2}\} = \{L, H\}$$

$(uz = \overline{1, n_{rs}}, ac = \overline{1,2})$, where: *L* – «Low» = 0,77; *H* – «High» = 0,44,

$\boldsymbol{PR}_{uz}$ – compliance with the authority represented by the plural

$$\boldsymbol{PR}_{uz} = \{\bigcup_{pr=1}^{3} PR_{uz,pr}\} =$$

$$\{PR_{uz,1}, PR_{uz,2}, PR_{uz,3}\} = \{N, L, H\}$$

$(uz = \overline{1, n_{rs}},\ pr = \overline{1,3})$, where: N – «Absent» = 0,85;

$$L - \text{«Low»} = \begin{cases} 0,62 \ at \ S_{uz,1} = U, \\ 0,68 \ at \ S_{uz,2} = C, \end{cases}$$ with

$\boldsymbol{S}_{uz}$ – action scope, which can be represented as a set

$$\boldsymbol{S}_{uz} = \{\bigcup_{s=1}^{2} S_{uz,s}\} = \{S_{uz,1}, S_{uz,2}\} = \{U, C\}$$

$(uz = \overline{1, n_{rs}}, s = \overline{1,2})$, where: U – «No changes»; C – «Changing»);

$$H - \text{«High»} = \begin{cases} 0,27 \ at \ S_{uz,1} = U, \\ 0,50 \ at \ S_{uz,2} = C, \end{cases}$$

$\boldsymbol{UI}_{uz}$ – user interaction, represented by the set

$$\boldsymbol{UI}_{uz} = \{\bigcup_{ui=1}^{2} UI_{uz,ui}\} = \{UI_{uz,1}, UI_{uz,2}\} = \{N, R\}$$

$(uz = \overline{1, n_{rs}}, ui = \overline{1,2})$, where: N – «No need» = 0,85; R – «Is required» = 0,62,

$\boldsymbol{C}_{uz}$ – impact on privacy, defined as a set

$$\boldsymbol{C}_{uz} = \{\bigcup_{c=1}^{3} C_{uz,c}\} = \{C_{uz,1}, C_{uz,2}, C_{uz,3}\} = \{N, L, H\}$$

$(uz = \overline{1, n_{rs}}, c = \overline{1,3})$, where: N – «Absent» = 0; L – «Low» = 0,22; H – «High» = 0,56,

$\boldsymbol{I}_{uz}$ – influence on integrity, which is represented by the set

$$\boldsymbol{I}_{uz} = \{\bigcup_{in=1}^{3} I_{uz,in}\} = \{I_{uz,1}, I_{uz,2}, I_{uz,3}\} = \{N, L, H\}$$

$(uz = \overline{1, n_{rs}}, in = \overline{1,3})$, where: N – «Absent» = 0; L – «Low» = 0,22; H – «High» = 0,56,

$\boldsymbol{A}_{uz}$ – the impact on availability, which can be represented by the plural

$$\boldsymbol{A}_{uz} = \{\bigcup_{ai=1}^{3} A_{uz,ai}\} = \{A_{uz,1}, A_{uz,2}, A_{uz,3}\} = \{N, L, H\},$$

$(uz = \overline{1, n_{rs}}, ai = \overline{1,3})$, where: N – «Absent» = 0; L – «Low» = 0,22; H – «High» = 0,56;

$\boldsymbol{T}$ – **temporal estimates**, which in accordance with paragraph 4.6 are presented as a set

$$\boldsymbol{T} = \{\bigcup_{uz=1}^{n_{rs}} T_{uz}\} \ (uz = \overline{1, n_{rs}}),$$

whose members are determined by a group of sets of parameters: $\boldsymbol{EX}_{uz}$, $\boldsymbol{RL}_{uz}$, $\boldsymbol{RC}_{uz}$ $(uz = \overline{1, n_{rs}})$, where:

$\boldsymbol{EX}_{uz}$ – usability, which can be displayed as a set

$$\boldsymbol{EX}_{uz} = \{\bigcup_{ex=1}^{5} EX_{uz,ex}\} = \{EX_{uz,1}, ..., EX_{uz,5}\} = \{X, U, POC, F, H\}$$

$(uz = \overline{1, n_{rs}},\ ex = \overline{1,5})$, where: X – «No data» = 1; U – «Theoretical (no evidence)» = 0,91; POC – «Experimental» = 0,94; F – «Functional» = 0,97; H – «High» = 1,

$\boldsymbol{RL}_{uz}$ – the level of correction (indicator of the degree of readiness of the decision), which is determined as a set

$$\boldsymbol{RL}_{uz} = \{\bigcup_{rl=1}^{5} RL_{uz,rl}\} = \{RL_{uz,1}, ..., RL_{uz,5}\} = \{X, OF, TF, W, U\}$$

$(uz = \overline{1, n_{rs}}, rl = \overline{1,5})$, where: X – «No data» = 1; OF – «Official patch» = 0,95; TF – «Interim solution» = 0,96; W – «Solutions based on tips and tricks» = 0,97; U – «Absent» = 1,

$\boldsymbol{RC}_{uz}$ – the reliability of the report (an indicator of the degree of reliability of information), which is represented by the set

$$\boldsymbol{RC}_{uz} = \{\bigcup_{rc=1}^{4} RC_{uz,rc}\}$$

$$= \left\{RC_{uz,1}, ..., RC_{uz,4}\right\} = \{X, U, R, C\}$$

$(uz = \overline{1, n_{rs}},\ rc = \overline{1,4})$, where: X – «No data» = 1; U – «Undefined» = 0,92; R – «Justified» = 0,96; C – «Confirmed» = 1;

E – **environmental metrics (Environmental)**, presented as a set

$$\boldsymbol{E} = \{\bigcup_{uz=1}^{n_{rs}} E_{uz}\} \ \ (uz = \overline{1, n_{rs}}),$$

whose members are determined by a group of sets of parameters: $\boldsymbol{CR}_{uz}$, $\boldsymbol{IR}_{uz}$, $\boldsymbol{AR}_{uz}$, $\boldsymbol{MS}_{uz}$, $\boldsymbol{MAV}_{uz}$, $\boldsymbol{MAC}_{uz}$, $\boldsymbol{MPR}_{uz}$, $\boldsymbol{MUI}_{uz}$, $\boldsymbol{MC}_{uz}$, $\boldsymbol{MI}_{uz}$, $\boldsymbol{MA}_{uz}$ $(uz = \overline{1, n_{rs}})$, where:

$\boldsymbol{CR}_{uz}$ – confidentiality requirements defined as a set

$$\boldsymbol{CR}_{uz} = \{\bigcup_{cr=1}^{4} CR_{uz,cr}\} =$$

$$\left\{CR_{uz,1}, ..., CR_{uz,4}\right\} = \left\{X, L, M, H\right\}$$

$(uz = \overline{1, n_{rs}},\ \ cr = \overline{1,4})$, where: X – «Undefined» = 1; L – «Low» = 0,5; M – «Medium» = 1; H – «High» = 1,5,

$\boldsymbol{IR}_{uz}$ – integrity requirements represented by the set

$$\boldsymbol{IR}_{uz} = \{\bigcup_{ir=1}^{4} IR_{uz,ir}\} = \{IR_{uz,1}, ...,$$

$$IR_{uz,4}\} = \left\{X, L, M, H\right\}$$

$(uz = \overline{1, n_{rs}},\ ir = \overline{1,4})$, where: X – «Undefined» = 1; L – «Low» = 0,5; M – «Medium»= 1; H – «High» = 1,5,

$\boldsymbol{AR}_{uz}$ – accessibility requirements, presented in the form of a set

$$\boldsymbol{AR}_{uz} = \{\bigcup_{ar=1}^{4} AR_{uz,ar}\} =$$

$$\left\{AR_{uz,1}, ..., AR_{uz,4}\right\} = \left\{X, L, M, H\right\}$$

$(uz = \overline{1, n_{rs}},\ \ ar = \overline{1,4})$, where: X – «Undefined» = 1; L – «Low» = 0,5; M – «Medium» = 1; H – «High» = 1,5,

$\boldsymbol{MS}_{uz}$ – modified action scope, which can be represented as a set

$$\boldsymbol{MS}_{uz} = \{\bigcup_{ms=1}^{3} MS_{uz,ms}\}$$

$$= \left\{MS_{uz,1}, MS_{uz,2}, MS_{uz,3}\right\} = \left\{X, U, C\right\}$$

$(uz = \overline{1, n_{rs}},\ ms = \overline{1,3})$, where: X – «Undefined»; U – «Unchanged»; C – «Changing»,

$\boldsymbol{MAV}_{uz}$ – modified cyber-attack vector, which is represented as a set

$$\text{Medium } \boldsymbol{MAV}_{uz} = \{\bigcup_{mav=1}^{5} MAV_{uz,mav}\}$$

$$= \left\{MAV_{uz,1}, ..., MAV_{uz,5}\right\} =$$

$$\left\{X, N, A, L, P\right\}$$

$(uz = \overline{1, n_{rs}},\ mav = \overline{1,5})$, where: X – «Undefined» = 1; N – «Network» = 0,85; A – «Connected network» = 0,62; L – «Local access» = 0,55; P – «Physical access» = 0,2,

$\boldsymbol{MAC}_{uz}$ – modified complexity of a cyberattack determined by the set

$$\boldsymbol{MAC}_{uz} = \{\bigcup_{mac=1}^{3} MAC_{uz,mac}\} =$$

$$\left\{MAC_{uz,1}, MAC_{uz,2}, MAC_{uz,3}\right\}$$

$$= \left\{X, L, H\right\}$$

$(uz = \overline{1, n_{rs}},\ mac = \overline{1,3})$, where: X – «Undefined» = 1; L – «Low» = 0,77; H – «High» = 0,44,

$\boldsymbol{MPR}_{uz}$ – modified compliance with the authority represented by the set

$$\boldsymbol{MPR}_{uz} = \{\bigcup_{mpr=1}^{4} MPR_{uz,mpr}\} =$$

$$\{MPR_{uz,1}, MPR_{uz,2},$$

$$MPR_{uz,3}, MPR_{uz,4}\} = \left\{X, N, L, H\right\}$$

$(uz = \overline{1, n_{rs}},\ \ mpr = \overline{1,4})$, where: X – «Undefined» = 1; N – «Absent» = 0,85;

$$L \text{ – «Low»} = \begin{cases} 0,62 \ at \ MS_{uz,1} = U, \\ 0,68 \ at \ MS_{uz,2} = C; \end{cases}$$

$$H - \text{«High»} = \begin{cases} 0,27 \; at \; MS_{uz,1} = U, \\ 0,50 \; at \; MS_{uz,2} = C, \end{cases}$$

$\boldsymbol{MUI}_{uz}$ – modified interaction with the user, represented by the set

$$\boldsymbol{MUI}_{uz} = \{\bigcup_{mui=1}^{3} MUI_{uz,mui}\} = \{MUI_{uz,1}, MUI_{uz,2}, MUI_{uz,3}\} = \{X, N, R\}$$

$(uz = \overline{1, n_{rs}}, mui = \overline{1,2})$, where: X – «Undefined» = 1; N – «No need» = 0,85; R – «There is a need» = 0,62,

$\boldsymbol{MC}_{uz}$ – modified impact on privacy determined by the set

$$\boldsymbol{MC}_{uz} = \{\bigcup_{mc=1}^{4} MC_{uz,mc}\} = \{MC_{uz,1}, MC_{uz,2}, MC_{uz,3}, MC_{uz,4}\} = \{X, N, L, H\}$$

$(uz = \overline{1, n_{rs}}, mc = \overline{1,4})$, where: X – «Undefined» = 1; N – «Absent» = 0; L – «Low» = 0,22; H – «High» = 0,56,

$\boldsymbol{MI}_{uz}$ – modified effect on the integrity determined by the set

$$\boldsymbol{MI}_{uz} = \{\bigcup_{min=1}^{4} MI_{uz,min}\} = \{MI_{uz,1}, MI_{uz,2}, MI_{uz,3}, MI_{uz,4}\} = \{X, N, L, H\}$$

$(uz = \overline{1, n_{rs}}, min = \overline{1,4})$, where: X – «Undefined» = 1; N – «Absent» = 0; L – «Low» = 0,22; H – «High» = 0,56,

$\boldsymbol{MA}_{uz}$ – modified effect on availability, represented by the set

$$\boldsymbol{MA}_{uz} = \{\bigcup_{mai=1}^{4} MA_{uz,mai}\} = \{MA_{uz,1}, MA_{uz,2}, MA_{uz,3}, MA_{uz,4}\} = \{X, N, L, H\}$$

$(uz = \overline{1, n_{rs}}, mai = \overline{1,4})$, where: X – «Undefined» = 1; N – «Absent» = 0; L – «Low» = 0,22; H – «High» = 0,56.

Next, we introduce the logical variable (LV) "LEVEL OF EVALUATION PARAMETER $\boldsymbol{EP}_i$" ($\boldsymbol{K}_{EP_i}$), which is determined by the tuple [2, 3] $< \boldsymbol{K}_{EP_i}, \underset{\sim}{T}_{K_{EP_i}}, \boldsymbol{X}_{EP_i} >$, where the base term sets are initialized by m-terms $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{K_{EP_i j}}$, for which, respectively, determine their intervals of values for each $\boldsymbol{EP}_i$, $(i = \overline{1, g})$ – $[k_{EP_i 1};\ k_{EP_i 2}[$, $[k_{EP_i 2};\ k_{EP_i 3}[$, …, $[k_{EP_i j-1};\ k_{EP_i j}[$, $[k_{EP_i j};\ k_{EP_i j+1}[$, …, $[k_{EP_i m};\ k_{EP_i m+1}]$.

Next, using the appropriate method [4], which is implemented using four stages, the conversion of intervals into fuzzy numbers (FN) – $\underset{\sim}{T}_{K_{EP_i j}} = (ai_j; bi_{1j}; bi_{2j}; ci_j)$.

To do this, we modify the expression of the method using the following redefinitions [4]: $a_j = b_{2j}$, $c_j = b_{1j}$, where $j = \overline{1, m}$, (m – number of term sets) $a_1 = b_{11} = 0$ i $c_m = b_{2m} = k_{m+1}$.

Significance assessment of $\boldsymbol{EP}_i$ is performed using parameters from the set $\boldsymbol{LS} \in \{LS_i\}$ $(i = \overline{1, g})$, and estimation of the current value of the estimation parameter – by means of set $\boldsymbol{ep} \in \{ep_{uz,i}\}$ $(uz = \overline{1, n_{rs}}, i = \overline{1, g})$.

Step 4 (Determining the number of term sets)

The number of term sets that will be used in the RA process is determined. If necessary, the initial number of term sets can be changed. For this purpose, for the equivalent transformation of m-dimensional terms of FN LV $\boldsymbol{DR}^{(m)}$ in $\boldsymbol{DR}^{(m-n)}$ or $\boldsymbol{DR}^{(m+n)}$ and $\boldsymbol{K}_{EP_i}^{(m)}$ in $\boldsymbol{K}_{EP_i}^{(m-n)}$ or $\boldsymbol{K}_{EP_i}^{(m+n)}$ it is proposed to use methods of realization of function of transformation of LV standards [5].

Step 5 (Assessment of the evaluation parameters significance level). This step is interrelated with a similar step of the method described in [5].

Step 6 (Determination of reference values of the risk degree).

In this step, the reference values for LV ***DR*** are determined, that is, the number of terms in the base term set is specified $\underset{\sim}{\boldsymbol{T}}_{DR}$, where they correspond to a given range of values in the range from dr_{min} to dr_{max}.

Step 7 (Determination of evaluation parameters reference values).

Experts determine the standards of parameters for LV $\boldsymbol{K}_{EP_i}$, that is, the number of terms in the term set $\underset{\sim}{\boldsymbol{T}}_{K_{EP_i}}$ is specified.

To convert intervals into FN, we use the method proposed in [5], which is implemented using four stages. For convenience of estimation parameters display through FN tab. 1 was used.

Table 1

Determination of FN values of estimation parameters

$\boldsymbol{EP}_i$	FN $\underset{\sim}{T}_{K_{EP_i j}} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$ for $\underset{\sim}{T}_{K_{EP_i 1}}$ – $\underset{\sim}{T}_{K_{EP_i m}}$, ($j = \overline{1,m}$)				
	$\underset{\sim}{T}_{K_{EP_i 1}}$	…	$\underset{\sim}{T}_{K_{EP_i j}}$	…	$\underset{\sim}{T}_{K_{EP_i m}}$
$\boldsymbol{EP}_1$	($a1_1$; $b1_{11}$; $b1_{21}$; $c1_1$)	…	($a1_j$; $b1_{1j}$; $b1_{2j}$; $c1_j$)	…	($a1_m$; $b1_{1m}$; $b1_{2m}$; $c1_m$)
…	…	…	…	…	…
$\boldsymbol{EP}_i$	(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)

Step 8 (Estimation of current parameter values)

For each evaluation parameter

$$\{\bigcup_{i=1}^{3} \boldsymbol{EP}_i\} = \{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_3\} = \{ \boldsymbol{B},\ \boldsymbol{T},\ \boldsymbol{E} \}\ (i = \overline{1,3})$$

determined $ep_{uz,i}$ $\forall V_{rs,uz}$, ($rs = \overline{1,ro}$, $uz = \overline{1,n_{rs}}$), that is $\{ep_{uz,i}\} = \{ep_{uz,\boldsymbol{B}}, ep_{uz,\boldsymbol{T}}, ep_{uz,\boldsymbol{E}}\}$.

The value of each of the parameters can be taken from known databases or determined by appropriate formulas [1]:

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

where $roundUp_1(\,)$ – function for rounding to the first decimal place (for example, 3,822 will be rounded to 3.8);

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

where

$$ISC_{uz} = 1 - ((1 - C_{uz,c})(1 - I_{uz,in})(1 - A_{uz,ai})),$$

values $S_{uz,s}$, $C_{uz,c}$, $I_{uz,in}$, $A_{uz,ai}$ we obtain on the basis of step 3 of this method, and

$$EXb_{uz} = 8{,}22 AV_{uz,av} AC_{uz,ac} PR_{uz,pr} UI_{uz,ui},$$

$$T_{uz} = roundUp_1(B_{uz} EX_{uz,ex} RL_{uz,rl} RC_{uz,rc}),$$

where the values $EX_{uz,ex}$, $RL_{uz,rl}$ i $RC_{uz,rc}$ also obtained on the basis of step 3 of the method;

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

where:

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

a $MEXb_{uz} = 8,22MAV_{uz,mav} \; MAC_{uz,mac} \; MPR_{uz,mpr} MUI_{uz,mui}$ i

$$MISC_{uz} = \min[(1-(1-MC_{uz,mc}CR_{uz,cr}) \; (1-MI_{uz,min}IR_{uz,ir}) \; (1-MA_{uz,mai}AR_{uz,ar})), \; 0,915],$$

while values $MS_{uz,ms}$, $MAV_{uz,mav}$, $MAC_{uz,mac}$, $MPR_{uz,mpr}$, $MUI_{uz,mui}$, $MC_{uz,mc}$, $CR_{uz,cr}$, $MI_{uz,min}$, $IR_{uz,ir}$, $MA_{uz,mai}$, $AR_{uz,ar}$ pre-defined in step 3 of this method. Here E_{uz} is a corrective evaluation parameter that determines B_{uz} and T_{uz}.

For clarity, the results of the calculations are entered in table. 2, where $\lambda_{uz,ij}$ – the level of affiliation of the carrier $ep_{uz,i}$ to the fuzzy subset $\underset{\sim}{T}_{K_{EP_i}j}$.

Similar transformations are carried out for all $V_{rs,uz}$.

Table 2

Classification of current values of evaluation parameters

EP_i	$\lambda_{uz,ij}$ for $\underset{\sim}{T}_{K_{EP_i}j}$ $(uz=\overline{1,n_{rs}}, \; i=\overline{1,g}, \; j=\overline{1,m})$				
	$\underset{\sim}{T}_{K_{EP_i}1}$	…	$\underset{\sim}{T}_{K_{EP_i}j}$	…	$\underset{\sim}{T}_{K_{EP_i}m}$
EP_1	$\lambda_{uz,11}$	…	$\lambda_{uz,1j}$	…	$\lambda_{uz,1m}$
…	…	…	…	…	…
EP_i	$\lambda_{uz,i1}$	…	$\lambda_{uz,ij}$	…	$\lambda_{uz,im}$
…	…	…	…	…	…
EP_g	$\lambda_{uz,g1}$	…	$\lambda_{uz,gj}$	…	$\lambda_{uz,gm}$

Step 10 (Risk degree assessment)

This step calculates the risk indicators for each vulnerability reflected by the identifier $V_{rs,uz}$ according to the formula

$$LRV_{rs,uz} = \sum_{j=1}^{m}\left(K_{lr_j} \sum_{i=1}^{g}(ks \cdot LS_i)\lambda_{uz,ij} \right),$$

where K_{lr_j} = 90 – 20(*m* – *j*), $ks = \dfrac{1}{(LS_1 + ... + LS_i)}$ – rationing factor, $\lambda_{uz,ij}$ $(uz=\overline{1,n_{rs}}, \; i=\overline{1,g}, \; j=\overline{1,m},)$ determined for each $V_{rs,uz}$ $(rs=\overline{1,ro}, \; uz=\overline{1,n_{rs}})$, and *LS*$_i$, $(i=\overline{1,g})$ depending on the significance of the parameter.

Step 11 (Formation of a structured risk parameter)

Based on the calculated value of $LRV_{rs,uz}$ and constructed standards form a structured parameter of the risk degree ***RD*** by expression:

$$SP_{uz} = \begin{cases} (LRV_{rs,uz}; \underset{\sim}{T}_{DR_j}) \\ at \; \mu_j(LRV_{rs,uz}) = 1; \\ (LRV_{rs,uz}; \underset{\sim}{T}_{DR_j}(\mu_j(LRV_{rs,uz})); \\ \underset{\sim}{T}_{DR_{j+1}}(\mu_{j+1}(LRV_{rs,uz}))) \\ at \; \mu_j(LRV_{rs,uz}) \neq 1 \wedge \mu_{j+1}(LRV_{rs,uz}) \neq 1, \end{cases}$$

where $(LRV_{rs,uz}; \underset{\sim}{T}_{DR_j})$ verbally interpreted as – «The risk degree $\underset{\sim}{T}_{DR_j}$ with a numerical equivalent $LRV_{rs,uz}$», and $(LRV_{rs,uz}; \underset{\sim}{T}_{DR_j}(\mu_j(LRV_{rs,uz}));$ $\underset{\sim}{T}_{DR_{j+1}}(\mu_{j+1}(LRV_{rs,uz})))$, as – «The risk degree with a numerical equivalent $LRV_{rs,uz}$, which borders $\underset{\sim}{T}_{DR_j}$ and $\underset{\sim}{T}_{DR_{j+1}}$ along the border

$\underset{\sim}{T}_{DR_j}$ – $\mu_j(LRV_{rs,uz})$ and $\underset{\sim}{T}_{DR_{j+1}}$ – $\mu_{j+1}(LRV_{rs,uz})$».

With the help of ***RD*** both the numerical value of the degree of risk and its linguistic interpretation can be obtained.

Also, can be calculated the average value LR_{rs} by estimation resource:

$$LR_{rs} = (\sum_{uz=1}^{n_{rs}} LRV_{rs,uz}) / n_{rs}.$$

Thus, the presented method of assessing the risks of IS based on open database vulnerabilities by modifying the procedures for determining the set of RA parameters and estimating the current values of parameters with the possibility of integration (as an alternative to expert estimates) of CVSS values (version 3.0) presented in NVD distinguish between vulnerable and offensive components, and also allows for the implementation of operational assessment and monitoring (real-time) of risks without the involvement of experts in the relevant subject area.

3. Information security risks assessment system

On the basis of the developed method the corresponding system of IS RA which due to use of structural components of subsystems of formation of primary and secondary data, and also components of their modules of initialization of input data, formation and transformation of reference values, weighing of estimation parameters and their adjustment, estimation of RD and generation of report, which implemented the proposed method, allows to provide certain properties of adaptability and efficiency in RA of RIS security in real time. Such a system, using CVSS metrics, allows to perform RA in real time, as well as at the request of the user to transform the reference LV without the involvement of specialists in the relevant field. In addition, the system provides the function of editing these metrics, using the built-in CVSS-calculator version 3.0 [1].

The structural solution of the proposed system (Fig. 1) consists of two basic components that reflect the subsystems of primary (SPDP) and secondary data (SSDP) processing. We describe the composition of each of the subsystems.

The SPDP subsystem is intended for primary processing of initial values and includes the module of input data initialization (MDI), and also modules of formation (MFR) and conversion (MCR) of reference values.

The SSDP subsystem, using CVSS metrics, performs the transformation of the primary parameters coming from the SPDP in order to form the final estimates of the RD. It consists of a module for weighing evaluation parameters (MWP) and their adjustment (MAP), as well as modules for estimating RD (MRD) and generating a report (MGR).

Let's consider the functional purpose of each of the modules of the subsystems. Thus, MDI is designed to form and identify many RIS and vulnerabilities of the evaluation object.

Here based on the set ***RIS*** for the specified object experts determine the required set of ***RIS*** (and, accordingly, their identifiers) $\boldsymbol{RISO} = \{\bigcup_{rs=1}^{ro} \boldsymbol{RISO}_{rs}\}$ $(rs = \overline{1, ro})$, where ro – the number of assessed ***RIS*** at the facility.

Next, for every $\boldsymbol{RISO}_{rs}$ determined the sets of their vulnerabilities $\{\bigcup_{rs=1}^{ro} \boldsymbol{V}_{rs}\} = \{\bigcup_{rs=1}^{ro}\{\bigcup_{uz=1}^{n_{rs}} V_{rs,uz}\}\}$ $(rs = \overline{1, ro},\ uz = \overline{1, n_{rs}})$, where n_{rs} – the possible number of identified vulnerabilities of rs-th estimated RIS $(\boldsymbol{RISO}_{rs})$.

As input for the MDI can be used, for example, the results of the program to check the system for penetration (Penetration test).

Such software, as a rule, analyzes the specified object, searching for vulnerabilities of its RIS in cyberspace (according to ISO / IEC 27032: 2012, cyberspace can be understood as a complex entity that actually exists as a global set of processes of interaction of people, software and Internet services in networks (including technological equipment connected to them), but which does not manifest itself in any known, material form).

Thus, a list is formed in the form of a set of RIS vulnerabilities of the studied object. To obtain a set of RIS and a set of relevant vulnerabilities in MDI, performed the processing

of the corresponding report obtained from specialized software (level - Penetration test), which contains information about RIS and vulnerabilities with the specified CVSS metrics.

Next, the list of vulnerabilities and RIS is initialized for further transmission to the MFR. As a result of the work of the MDI, all identified MFRs arrive at the entrance $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$ and their CVSS metrics.

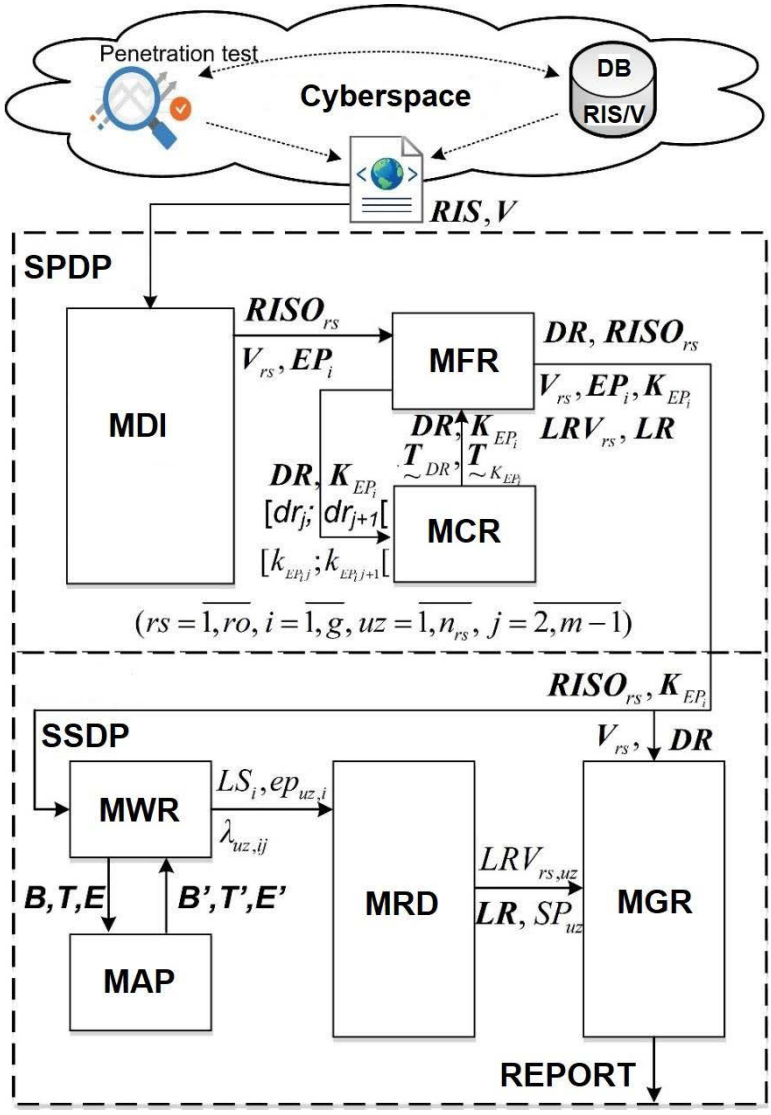

Figure 1: Structural solution of the IS RA system in real time

Next, the MFR performs the formation of a set of parameters:

– $\boldsymbol{LR} = \{\bigcup_{rs=1}^{ro} \boldsymbol{LR}_{rs}\}$ $(rs = \overline{1,ro})$,

where $\boldsymbol{LR}_{rs}$ – quantitative risk assessment of rs – th RIS on object (used for $\boldsymbol{RISO}_{rs}$);

– $\boldsymbol{LRV} = \{\bigcup_{rs=1}^{ro} \boldsymbol{LRV}_{rs}\} = \{\bigcup_{rs=1}^{ro} \{\bigcup_{uz=1}^{n_{rs}} LRV_{rs,uz}\}\}$ $(rs = \overline{1,ro}, uz = \overline{1,n_{rs}})$, where $LRV_{rs,uz}$ – quantitative risk assessment for each uz – th vulnerability of rs – th RIS on the object (used for the RA for each vulnerability reflected by the identifier $V_{rs,uz}$);

– $\boldsymbol{DR}$, where LV «RISK DEGREE» is represented as a corresponding tuple <$\boldsymbol{DR}$, $\underset{\sim}{T}_{DR}$, $\boldsymbol{X}_{DR}$> (is used to display the RA result);

– $\boldsymbol{EP} = \{\bigcup_{i=1}^{g} \boldsymbol{EP}_i\}$ $(i = \overline{1,g})$,

where g – number of sets of evaluation parameters

(used to ensure the evaluation process, based on CVSS indicators);

– $\boldsymbol{K}_{EP_i}$, where LV «LEVEL OF EVALUATION PARAMETER $\boldsymbol{EP}_i$» determined by the tuple $<\boldsymbol{K}_{EP_i}, \underset{\sim}{T}_{K_{EP_i}}, \boldsymbol{X}_{EP_i}>$ (used to display evaluation results using CVSS metrics).

Formed LVs ***DR*** and $\boldsymbol{K}_{EP_i}$ are transmitted to the input of the MCR, where for each of the terms $\underset{\sim}{T}_{DR_1}, \ldots, \underset{\sim}{T}_{DR_j}, \ldots, \underset{\sim}{T}_{DR_m}$ i $\underset{\sim}{T}_{K_{EP_i1}}, \underset{\sim}{T}_{K_{EP_i2}}, \ldots,$ $\underset{\sim}{T}_{K_{EP_ij-1}}, \underset{\sim}{T}_{K_{EP_ij}}, \ldots, \underset{\sim}{T}_{K_{EP_im}}$ the transformation is implemented according to the specified range of values $[dr_1; dr_2[, \ldots, [dr_j; dr_{j+1}[, \ldots, [dr_m; dr_{m+1}]$ i $[k_{EP_i1}; k_{EP_i2}[, [k_{EP_i2}; k_{EP_i3}[, \ldots, [k_{EP_ij-1}; k_{EP_ij}[, [k_{EP_ij}; k_{EP_ij+1}[, \ldots, [k_{EP_im}; k_{EP_im+1}]$ to FN. Also in MCR the procedure of variation by the order of LV is implemented. Thus, for the equivalent transformation of *m*-dimensional terms of FN LV $\boldsymbol{DR}^{(m)}$ to $\boldsymbol{DR}^{(m-n)}$ or $\boldsymbol{DR}^{(m+n)}$ and $\boldsymbol{K}_{EP_i}^{(m)}$ to $\boldsymbol{K}_{EP_i}^{(m-n)}$ or $\boldsymbol{K}_{EP_i}^{(m+n)}$ in MCR methods of transformation of LV standards are used. As a result of transformations on output of SPDP arrive $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$ and their CVSS metrics, $\boldsymbol{EP}_i$, LV ***DR*** and $\boldsymbol{K}_{EP_i}$, as well as formed sets $\boldsymbol{LR}$ i $\boldsymbol{LRV}_{rs}$ for RA.

Significance levels of estimation parameters are defined in MWP SSDP $LS_i \ (i=\overline{1,g})$ and their current values $\boldsymbol{ep}_{uz,i}$ from SPDP, for example, $\{\bigcup_{i=1}^{3} \boldsymbol{EP}_i\} = \{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_3\} = \{$ $\boldsymbol{B}, \boldsymbol{T}, \boldsymbol{E}\} \ (i=\overline{1,3})$.

Then, with the help of reference values, the process of fasification is carried out, which is associated with the determination of affiliation of $\boldsymbol{ep}_{uz,i}$ to a given FN, after which values $\lambda_{uz,ij}$ are formed. Also in MWP the graphic interpretation of estimation parameters is carried out ***B, T*** and ***E***.

If necessary, it is possible to adjust the CVSS metrics using the MAP, which implements their redefinition due to the built-in CVSS-calculator (see Fig. 2). Adjusted parameters ***B'***, ***T'*** and ***E'*** are transferred back to the MWP.

Data from MWP LS_i, $\boldsymbol{ep}_{uz,i}$ and $\lambda_{uz,ij}$ enter the MSP, where for each vulnerability reflected by the identifier $V_{rs,uz}$, SR evaluation is implemented $LRV_{rs,uz}$, and the average value is calculated $\boldsymbol{LR}_{rs}$ for RIS.

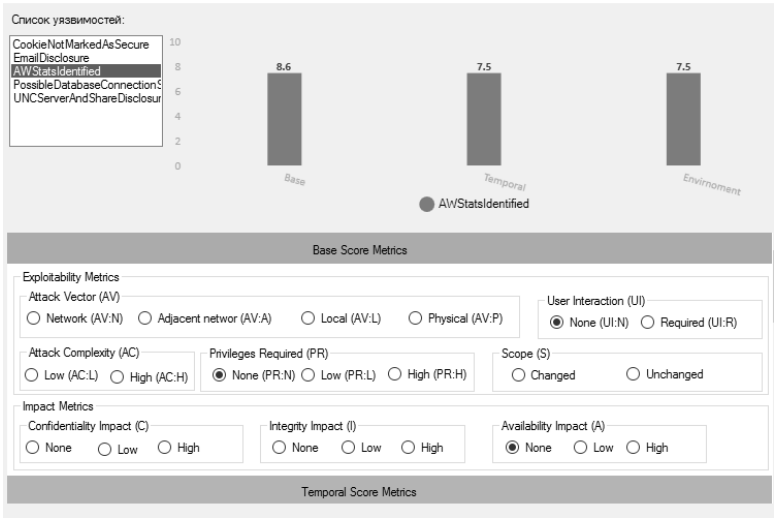

Figure 2: Built-in CVSS-calculator with graphical interpretation of CVSS metrics

Next, based on the calculated value $LRV_{rs,uz}$, $\boldsymbol{LR}_{rs}$ and constructed standards in the SPDP, the process of defasification, which is associated with the formation of a structured parameter of the RD SP_{uz}, which allows to obtain numerical values of RD and its linguistic interpretation.

On the basis of MGR, taking into account the results of SPDP and SSDP, a report is generated on the estimates of the RD (see Fig. 3), which

contains $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$, $LRV_{rs,uz}$, $\boldsymbol{LR}_{rs}$, their linguistic equivalents and graphical interpretation of the results.

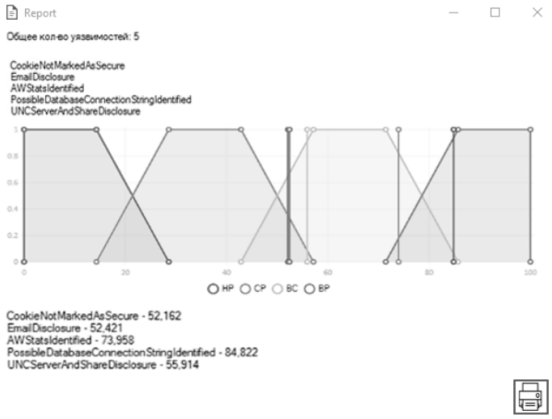

Figure 3: Example of the generated report

The proposed real-time IS RA system, for example, can be implemented programmatically and work on the basis of the proposed basic algorithm (Fig. 4).

According to this algorithm, the operation of the system begins with the initialization of the list of vulnerabilities and CVSS ratings (top 1) using a specialized program to check the system for penetration (Penetration test).

This procedure in the software implementation can, for example, be performed by the function OpenXMLFile (), which opens the file in XML format and implements its parsing. XML file parsing is used to initialize (fill in) fields in the Vulnerability class with the following structure:

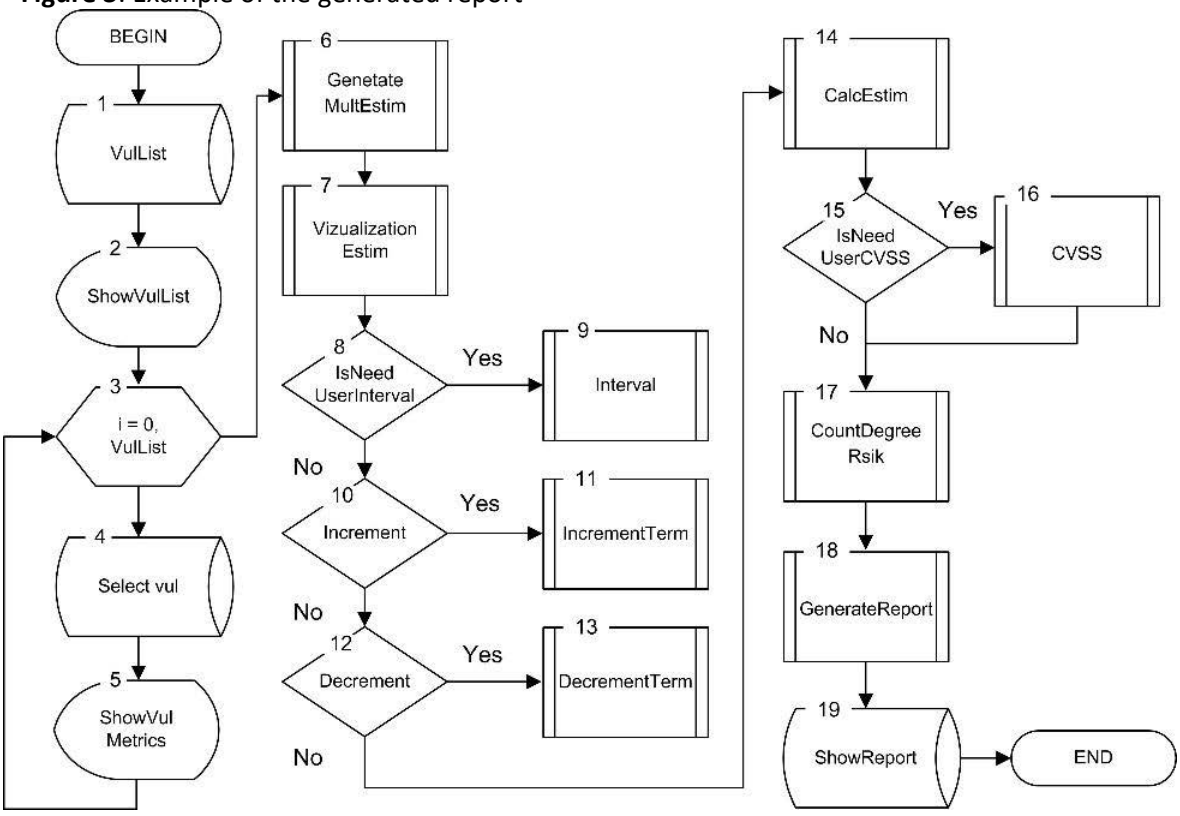

Figure 4: Basic algorithm of IS RA system operation

```
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();
    }}.
```

After identifying the next vulnerability (Vulnerability class), its characteristics are entered into the List container, resulting in the formation of a structure – List <Vulnerability>. Next, after generating a list of vulnerabilities (vertex 2), its contents are written to the ListBox component with $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$ and their CVSS estimates.

Next, in the loop (vertex 3) performs a selection of vulnerabilities (vertex 4) from the ListBox (Select Vul) and their graphical interpretation (vertex 5) CVSS metrics (Fig. 2). This process provides the appropriate event handler - the lbVul CVSS_

SelectedIndexChanged function. The moment the SelectedIndexChanged event occurs when the index of the selected ListBox component changes. The lbVulCVSS_SelectedIndexChanged function graphically displays CVSS metrics based on the LiveChart library. CVSS metrics are displayed in the form of a bar chart (see Fig. 2), which is achieved using the following block of program listing:

```
chartCVSS.Series.Add(new ColumnSeries()
        {
          Title =
vulList[lb.SelectedIndex].Description,
          Values = new
ChartValues<ObservableValue>()
          {
            new
ObservableValue(vulList[lb.SelectedIndex].metri
cs.baseVector.CommonScore),
            new
ObservableValue(vulList[lb.SelectedIndex].metri
cs.tempVector.CommonScore),
            new
ObservableValue(vulList[lb.SelectedIndex].metri
cs.envirVector.CommonScore)
          },
          DataLabels = true});
```

Next, with the help of a predetermined process (vertex 6) is the formation of LV $\boldsymbol{K}_{EP_i}$ and ***DR***, and sets are initialized for subsequent estimates $\boldsymbol{LR}$ and $\boldsymbol{LRV}_{rs}$.

After the formation of the necessary linguistic terms, the conversion of the given intervals into FN is performed, linguistic standards are formed and their graphical interpretation is realized (vertex 7). For clarity, the obtained CVSS metrics for each vulnerability are displayed on a graph with reference values $\boldsymbol{EP}_i$ (see Fig. 5).

Representation of terms of LV $\boldsymbol{K}_{EP_i}$ in graphical form (in accordance with the software implementation of the system) is provided by the structure of TrapezeCreator, which may have, for example, such fields:

```
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; }
  }.
```

The intervals that will be used to convert to FN are described by the Interval structure, which consists of the following fields:

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

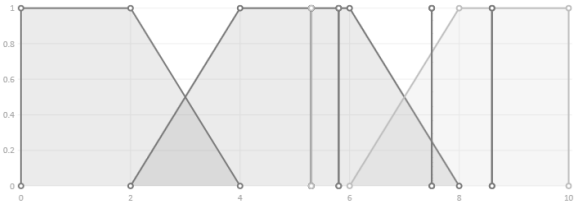

Figure 5: Graphical interpretation of the obtained CVSS metrics and standards of evaluation parameters

Graphical interpretation of the obtained results (according to the proposed software implementation) is carried out using the function List <Trapeze> CreateTrapezeList (double lengthAsixX, int countTrap, params double [] intervalArr). Next, with the help of subroutines Interval, IncrementTerm, DecrementTerm and conditional vertices (vertices 8-13), which are used to control the need for additional data processing, ie converting the specified intervals into FN, the process of decrementing and incrementing the order of LV.

Initialization of a new interval in the program is realized by means of the following block of program listing (verses 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;}.
```

Intervals are formed from a pre-formed list of intervalList, having the type List <Interval>, and are filled using the following block of program listing:

```
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 });}.
```

The procedure of incrementing (vertices 10-11) or decrementing (vertices 12-13) can be carried out, for example, using the developed functions List <Trapeze> IncrementTrapezeList (List <Trapeze> trapList, double lengthAsixX) or List <Trapeze> DecrementTrapezeList (List <Trapeze > trapList, double lengthAsixX).

On the basis of the received CVSS metrics the estimation (top 14) is realized LS_i and classification of $\lambda_{uz,ij}$ obtained $\boldsymbol{ep}_{uz,i}$ (fasification).

If necessary (vertex 15) CVSS metrics are adjusted ***B***, ***T*** and ***E*** (vertex 16). Next, using the data obtained LS_i and $\lambda_{uz,ij}$, estimated RD $LRV_{rs,uz}$ (vertex 17) for each vulnerability reflected by the identifier $V_{rs,uz}$, and the average value is calculated $\boldsymbol{LR}_{rs}$. Here, based on the received $LRV_{rs,uz}$, $\boldsymbol{LR}_{rs}$ and constructed standards in the PDP, the structured parameter RD is formed SP_{uz} (dephasification).

As a result of the calculations performed by the method of IS RA (vertex 18) a report is formed on the estimates of the RD (Fig. 6), which contains $\boldsymbol{RISO}_{rs}$, $\boldsymbol{V}_{rs}$, $LRV_{rs,uz}$, $\boldsymbol{LR}_{rs}$, their linguistic equivalents, as well as a graphical interpretation (vertex 19) of the results (Fig. 3). To verify the work of the developed software (see Fig. 6), a corresponding experimental study was conducted.

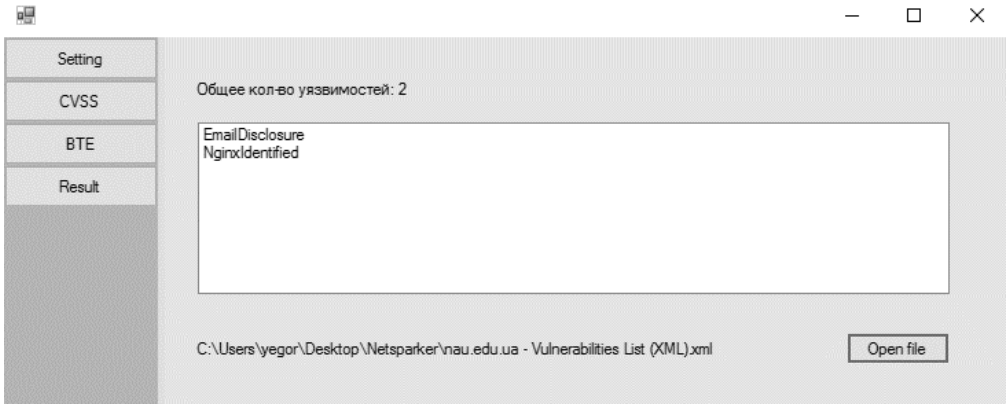

Figure 6: Fragment of the software system interface

To test the object of assessment for penetration used software to test the system for vulnerabilities - "Netsparker" (Fig. 7).

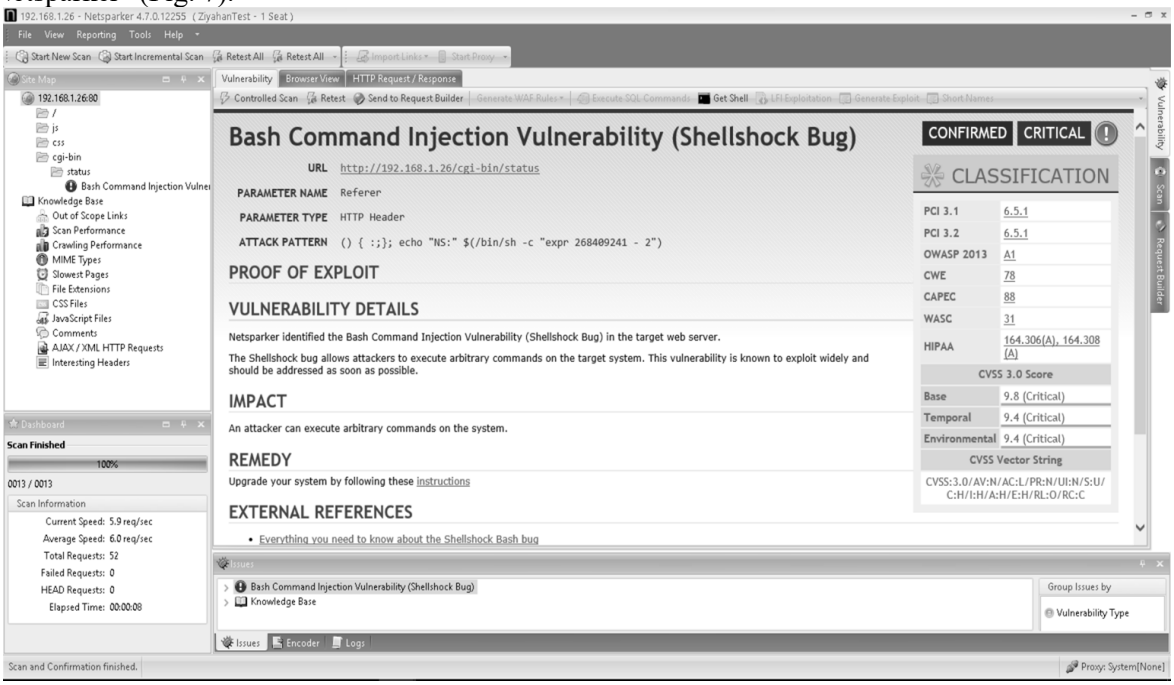

Figure 7: Interface part of the vulnerability scanning program «Netsparker»

As a result of scanning the XML file with the list of RIS and their vulnerabilities (fig. 8) was formed for the further use as input data of the developed system of IS RA.

xml-vul.txt — Блокнот

Файл Правка Формат Вид Справка

```
<classification>
        <OWASP2013></OWASP2013>
        <WASC>45</WASC>
        <CWE>200</CWE>
        <CAPEC>224</CAPEC>
        <PCI31></PCI31>
        <PCI32></PCI32>
        <HIPAA></HIPAA>
        <OWASPPC>C6</OWASPPC>

                <CVSS>
                        <vector>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N</vector>

                        <score>
                                <type>Base</type>
                                <value>7.5</value>
                                <severity>High</severity>
                        </score>
                        <score>
                                <type>Temporal</type>
                                <value>7.5</value>
                                <severity>High</severity>
                        </score>
                        <score>
                                <type>Environmental</type>
                                <value>7.5</value>
                                <severity>High</severity>
                        </score>

                </CVSS>
</classification>
```

Figure 8: XML file with a list of vulnerabilities

Next, the input data is initialized as a list of vulnerabilities in the ListBox.

In fig. 9 and fig. 10, respectively, visualized examples of the implementation of the function of transforming the order of LV ***DR,*** which is performed at the request of the user by activating the process of increment and decrement.

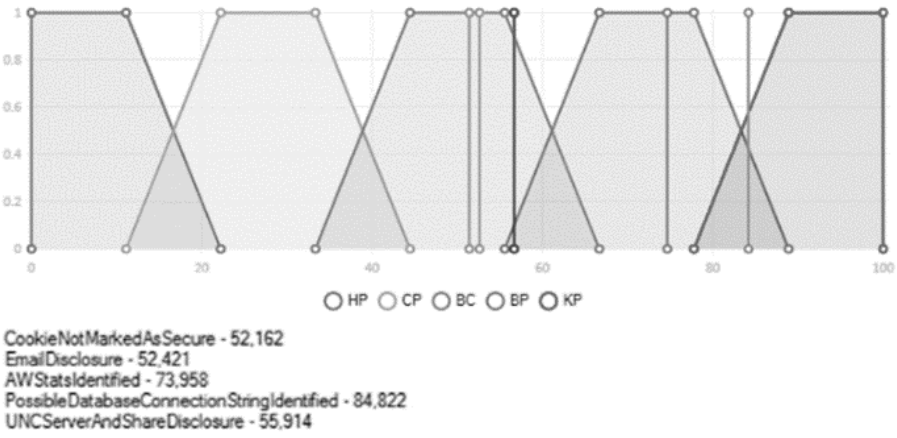

Figure 9: The result of incrementing the order of LV ***DR***

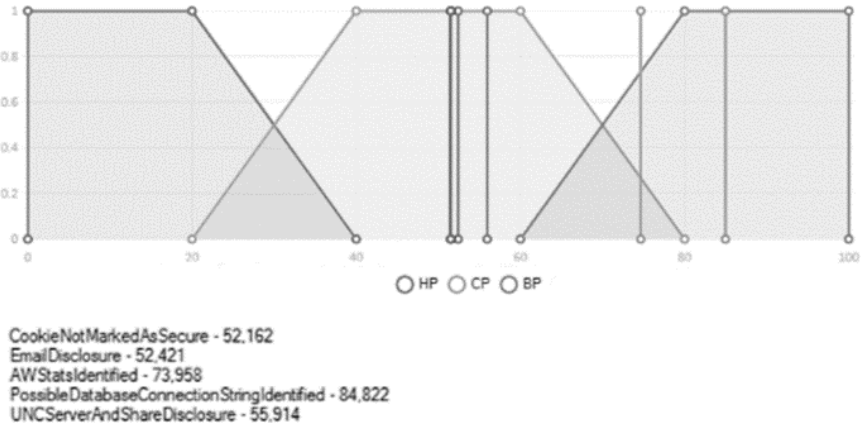

Figure 10: The result of decrement of LV ***DR***

Based on the obtained information about the assessment components and vulnerabilities, the system implements the calculation (vertex 17) of the RD for each vulnerability and with the help of a subprogram (vertex 18) that implements the functions of the MGR, performs a graphical interpretation of the vulnerability of the LV ***DR*** at m=4 (see Fig. 11). All the obtained results are recorded in the report generated by MGR.

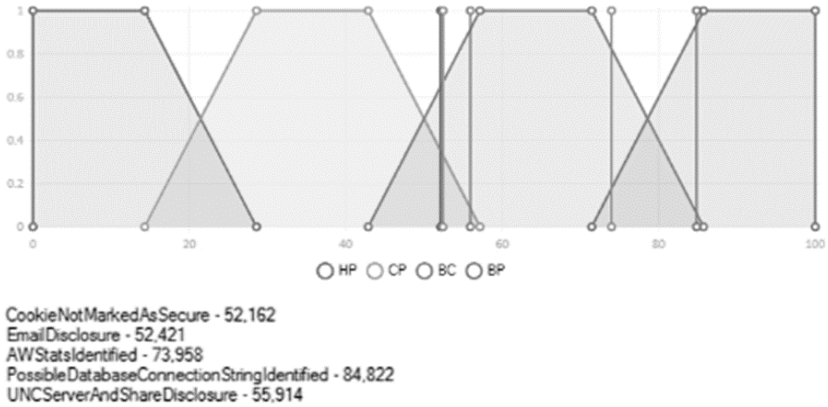

Figure 11: The result of the calculation of the RD for the identified vulnerabilities at the object of assessment

4. Conclusions

Thus, the structural solution of the real-time IS RA system is developed, which, due to the structural components of the subsystems of primary and secondary data generation, as well as their components of input data initialization modules, formation and conversion of reference values, weighing evaluation parameters and their adjustment, evaluation of RD and report generation, in which the proposed method is implemented, allows to provide certain properties of adaptability and efficiency in RA security of RIS in real time.

Also on the basis of the offered structural decision the basic algorithm and the corresponding software for estimation in the form of application software system of RA which unlike known uses values of CVSS (versions 2.0 and 3.0) of the indicators presented in the corresponding databases and allows real-time risk assessment of RIS security.

5. References

[1] «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/user-guide.

[2] A. Korchenko, A. Arkhypov, S. Kazmyrchuk, Analyz y otsenyvanye ryskov ynformatsyonnoi bezopasnosty. Monohrafyia, Kyev: OOO «Lazuryt-Polyhraf», 2013, s. 275. (А. Корченко, А. Архипов, С. Казмирчук, *Анализ и оценивание рисков информационной безопасности*. *Монография*, Киев: ООО «Лазурит-Полиграф», 2013, с. 275).

[3] A. Korchenko, Postroenye system zashchyty ynformatsyy na nechetkykh mnozhestvakh. Teoryia y praktycheskye reshenyia, K.: MK-Press, 2006, s.320. (А. Корченко, *Построение систем защиты информации на нечетких множествах. Теория и практические решения*, К.: МК-Пресс, 2006, с.320).

[4] A. Korchenko, S. Kazmyrchuk, «Metod preobrazovanyia yntervalov v nechetkye chysla dlia system analyza y otsenyvanyia ryskov», Pravovoe, normatyvnoe y metrolohycheskoe obespechenye systemы zashchyty ynformatsyy v Ukrayne, № 1(31), S. 57-64, 2016. (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).

[5] Korchenko O.H, Kazmirchuk S.V., Akhmetov B.B., Prykladni systemy otsiniuvannia ryzykiv informatsiinoi bezpeky, Monohrafiia. – K.: TsP «Komprynt», 2017. – 435 s. (Корченко О.Г, Казмірчук С.В., Ахметов Б.Б., Прикладні системи оцінювання ризиків інформаційної безпеки, Монографія. – К.: ЦП «Компринт», 2017. – 435 с.).