УДК 681.3:519.1

МЕТОДИКА КОЛИЧЕСТВЕННОЙ ОЦЕНКИ ВЕЛИЧИНЫ РИСКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ И СВЯЗИ

© 2016 С. А. Никулин*, С. С. Никулин**

** Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж), ул. Старых Большевиков, 54а, 394064, г. Воронеж, Россия*
*** Воронежский институт МВД России, проспект Патриотов, 53, 394065, г. Воронеж, Россия*
E-mail: nikcc@mail.ru

Поступила в редакцию 15.01.2016 г.

Аннотация. Рассматривается задача оценки рисков информационной безопасности автоматизированных систем управления и связи (АСУС) на основе использования теории нечетких множеств и нечеткой логики.
В работе построены функции принадлежности нечетких множеств с использованием экспертного метода последовательных интервалов. Рассмотрен пример оценки риска информационной безопасности от реализации угрозы создания боевым расчетом АСУС нештатных режимов функционирования программных (программно-аппаратных) средств с использованием алгоритма Мамдани.
Ключевые слова: риски информационной безопасности, угрозы безопасности информации, вероятность реализации угрозы, ущерб от реализации угроз, теория нечетких множеств и нечеткой логики, алгоритм Мамдани.

ВВЕДЕНИЕ

Широкое внедрение новых информационных технологий (ИТ) в процесс управления государством определяет особую актуальность создания подходов к надежному комплексному обеспечению информационной безопасности (ИБ) автоматизированных систем управления и связи органов государственной власти. Если качество защиты информации рассматривать с точки зрения рисков, то реализация таких подходов в настоящее время возможна путем создания систем защиты информации (СЗИ), важнейшим признаком которых является наличие управления рисками ИБ АСУС.

Целью процесса управления рисками является принятие и реализация таких управленческих решений, чтобы в течение заданного времени функционирования АСУС уровень риска соответствовал бы требуемому, а выделенные для этих целей ресурсы расходовались бы наиболее рациональным способом. Однако принятие решений на различных этапах процесса управления рисками ИБ АСУС характеризуется неполнотой и нечеткостью исходной информации. Для управления рисками ИБ требуется идентифицировать возможные опасности, угрожающие АСУС. В работе рассмотрены наиболее характерные умышленные угрозы нарушения основных состояний защищенности информации, в частности угрозы создания боевым расчетом АСУС нештатных режимов функционирования программных (программно-аппаратных) средств путем внесения преднамеренных изменений в данные, игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации, а также путем модификации самих данных.

МЕТОДИКА ЭКСПЕРИМЕНТА

В настоящее время имеется ряд нормативных документов, содержащих рекомендации по разработке эффективных систем управления рисками, среди которых актуальными являются: международный стандарт ISO/IEC 27005:2011 «Информационная технология. Методы и средства обеспечения безопасности. Управление рисками ИБ» и ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности.

Менеджмент риска информационной безопасности».

Все современные нормативные документы и стандарты в области ИБ отражают сложившийся в международной практике общий процессный подход к организации управления рисками. При этом управление рисками представляется как базовая часть системы менеджмента качества организации. Стандарты носят откровенно концептуальный характер, что позволяет экспертам по ИБ реализовать любые методы, средства и технологии оценки, отработки и управления рисками. В тоже время, стандарты не содержат рекомендаций по выбору какого-либо аппарата оценки риска, а также по синтезу мер, средств и сервисов безопасности, используемых для минимизации рисков, что снижает полезность стандартов как технологических документов.

Риски нужно контролировать постоянно, периодически проводя их переоценку. Целью оценки и переоценки является получение ответов на вопросы, приемлемы ли существующие риски, и если нет, то какие защитные средства экономически выгодно использовать. Кроме того, управление рисками – процесс далеко не линейный. Практически все его этапы связаны между собой, и по завершении любого из них может выявиться необходимость возврата к предыдущему.

В основе большинства методик риск (*Risk*) определяется исходя из двух факторов: вероятности реализации угрозы ($P_{\text{угр}}$) и ущерба ($C_{\text{ущ}}$), нанесенного информации от реализации угроз,

$$Risk = P_{\text{угр}} * C_{\text{ущ}}. \qquad (1.1)$$

Выражение (1.1) можно рассматривать как математическую формулу, если используются количественные шкалы, либо как формулировку общей идеи, если хотя бы одна из шкал – качественная. Из формулы (1.1) следует, что риск напрямую зависит от вероятности реализации угрозы. Единственной возможностью получения этих значений – получения субъективной вероятности по уровневым значениям этих показателей – является опрос экспертов [3; 8; 9].

При оценке риска ИБ АСУС необходимо учитывать динамический характер этих рисков, который проявляется в способности злоумышленников адаптироваться к изменению текущего состояния объекта, извлекать уроки из опыта предыдущих атак и реагировать на построение СЗИ путем корректировки сценариев осуществления атак с целью преодоления создаваемых барьеров и нанесения максимального ущерба.

В результате рассмотрения негативных воздействий различных типов для рассматриваемой АСУ может быть построен вектор, компонентами которого будут являться частные риски реализации атак разных типов

$$\vec{R}isk_S = \{Risk_1, Risk_2, \ldots, Risk_{SS}\}. \qquad (1.2)$$

Далее может быть определена норма этого вектора, взятая с некоторыми весами λ_i, $i = 1, 2, \ldots, SS$.

За норму вектора $(\overrightarrow{\lambda Risk}) = (\lambda_1 Risk_1, \lambda_2 Risk_2, \ldots, \lambda_{SS} Risk_{SS})^T$ в пространстве E^{SS} будем принимать норму [6]

$$L_p = \left\| Risk_S \right\| = \left[\sum_{i=1}^{SS} (\lambda_i Risk_i)^p \right]^{1/p}, \quad \lambda_i, Risk_i > 0, \qquad (1.3)$$

где $p \geq 1$ – показатель степени.

При $p = 1$ имеет место норма, представляющая собой сумму взвешенных показателей качества:

$$L_1 = \sum_{i=1}^{SS} \lambda_i Risk_i. \qquad (1.4)$$

При $p = 2$ норма L_2 имеем среднеквадратичную оценку

$$L_2 = \sqrt{\sum_{i=1}^{SS} (\lambda_i Risk_i)^2}. \qquad (1.5)$$

При увеличении степени p до бесконечности приходим к норме

$$L_\infty = \max_{1 \leq i \leq SS} \{\lambda_i Risk_i\}. \qquad (1.6)$$

Полученная по одной из формул (1.3) – (1.6) величина может быть использована как некоторая интегральная оценка риска ИБ для рассматриваемой АСУС.

Комплексный показатель защищенности АСУС может быть записан, например, в виде $Z = \dfrac{Risk_{\text{доп}}}{\left\| Risk_S \right\|}$, где $Risk_{\text{доп}}$ – установленный нормативный допустимый уровень риска ИБ для рассматриваемого объекта. Таким образом, полученный интегральный риск ИБ $\left\| \vec{R}isk_S \right\|$ может быть использован для оценки уровня защищенности рассматриваемой АСУС и обоснования необходимости реализации тех или иных мероприятий [3; 5; 10].

Одной из ключевых задач в процессе управления рисками является задача обоснования

требований к ИБ АСУС, которая сводится в рассматриваемом случае к определению нормативного допустимого уровня риска. Один из подходов к решению этой задачи заключается в следующем. Пусть имеется перечень (набор) негативных событий $\vec{A} = \{A_1, A_2, \ldots, A_n\}$, соответствующих атакам на АСУС. Тогда для данного набора $\vec{A}$ вероятностей реализации угроз $\vec{P}_A = \{P_{A1}, P_{A2}, \ldots, P_{An}\}$ и ущербов $\vec{C}_A = \{C_{A1}, C_{A2}, \ldots, C_{An}\}$ значение интегрального риска равно

$$Risk_S(\vec{A}, \vec{P}_A, \vec{C}_A) = \sum_{i=1}^{n} P_{Ai} \cdot C_{Ai}. \qquad (1.7)$$

Очевидно, что

$$Risk_S(\vec{A}, \vec{P}_A, \vec{C}_A) \Rightarrow \min. \qquad (1.8)$$

Так как $Risk_{S\min}(\vec{A}, \vec{P}_A, \vec{C}_A) \neq 0$, риск от реализации высоких и средних угроз принимают равным

$$Risk_{\text{доп}} = Risk_{S\min}(\vec{A}, \vec{P}_A, \vec{C}_A), \qquad (1.9)$$

и это значение $Risk_{\text{доп}}$ считают допустимым (или приемлемым) риском. Если $Risk_S(\vec{A}, \vec{P}_A, \vec{C}_A) \leq Risk_{\text{доп}}$, то АСУС относится к классу приемлемого риска, а если $Risk_S(\vec{A}, \vec{P}_A, \vec{C}_A) > Risk_{\text{доп}}$, то недопустимого риска.

Одним из подходов оценки вероятности реализации угроз и ущерба является применение аппарата нечетких множеств и нечеткой логики, который позволяет экспертным путем получить вероятностную меру этих показателей [2]. Механизм оценки риска информационной безопасности на основе нечеткой логики заключается в следующем:

1. Для входных переменных ($P_{\text{угр}}$ – «вероятность реализации угрозы», $C_{\text{ущ}}$ – «ущерб от реализации угрозы») и *Risk* – «риска» задаются шкалы, на которых определены нечеткие термы, соответствующие значениям переменных.

2. Определяется логика связи входных величин и «риска».

3. Определяются значения оценки входных переменных.

Аппарат нечеткой логики требует представления оценок показателей в виде нечетких переменных. Это достаточно сложная задача, однако в каждом конкретном случае могут быть найдены и обоснованы способы ее решения. Аппарат нечеткой логики допускает некоторую свободу в выборе алгоритмов обработки данных. Наиболее распространенным алгоритмом нечеткого вывода является алгоритм Мамдами, который позволяет получить из нечетких входных значений четкие выходные посредством использования принципа максимина.

Данный алгоритм используется для оценки и ранжирования информационных рисков по нескольким критериям, в соответствие которым ставятся нечеткие переменные (σ, X, Y), где σ – имя переменной, X – область определения σ, Y – нечеткое множество на X, которое может быть представлено набором функций принадлежности $\varphi_y(a)$. Множества X, Y определяются критерием «вероятность реализации», который соответствует нечеткой переменной. Такая переменная может быть описана несколькими значениями, например: «высокая», «средняя» и «низкая», при этом каждому значению будет соответствовать своя функция принадлежности, задаваемая с помощью треугольной, трапециевидной и экспоненциальной функций.

Механизм нечетких множеств и логики требует формирования определенных правил, конструкция которых имеет следующий вид:

Правило 1 : если a есть A_1 и b есть B_1, то c есть C_1;

Правило 2 : если a есть A_2 и в есть B_2, то c есть C_2;

…

Правило n : если a есть A_n и b есть B_n, то c есть C_n,

где a и b – входные переменные (вероятность угрозы и ущерб от ее реализации), c – переменная вывода (оценка риска), A_1, A_2,..., A_n, B_1, B_2,..., B_n, C_1, C_2,..., C_n – некоторые заданные функции принадлежности, при этом значение c_0 определяется на основе приведенной информации и четких значений a_0 и b_0.

Существует ряд методов построения по экспертным оценкам функций принадлежности нечеткого множества. Однако в большинстве случаев от экспертов проще получить информацию о размытости границ между соседними термами, т. е. информация может быть сосредоточена в функциях размытости границ термов $\varphi_{i,\,i+1}(a)$, $i = 1, 2, \ldots, n-1$. Оценка $\varphi_{i,\,i+1}(a)$ будет заключена в интервале Δa_i на физической шкале универсального множества X, соответствующего пересечению двух соседних термов X_i и X_{i+1}. На полученных в результате опроса интервалах $\Delta a_{i,j}$ строятся функции $\tau_{i,j}(a)$, вид которых выбирается из априорных соображений. Как правило, при отсутствии априорных сведений в качестве $\tau_{i,j}(a)$ выбирается прямоугольная функция единичной площади, которая от-

ражает индивидуальное мнение экспертов и имеет следующий вид:

$$\tau_{i,j} = \begin{cases} \dfrac{1}{\Delta a_{i,j}} \text{ при } a \subset \Delta a_{i,j}; \\ 0 \text{ при } a \not\subset \Delta a_{i,j}. \end{cases} \qquad (2.1)$$

Обобщенное мнение экспертов может быть представлено в виде

$$\phi_{i,i+1}(a) = \frac{\sum_{j=1}^{m} \tau_{i,j}(a)}{\max\limits_{a} \sum_{j=1}^{m} \tau_{i,j}(a)}, \qquad (2.2)$$

где знаменатель выполняет функцию нормировки, в результате которой $\max \varphi_{i,\,i+1}(a) = 1$.

Количество термов, описывающих переменную, может быть произвольным. Однако, при небольшом их количестве уменьшается точность оценки, а при слишком большом – увеличивается погрешность при экспертном опросе.

Для получения четкого значения выходной переменной «риск информационной безопасности» используется алгоритм Мамдани, который заключается в выполнении следующих этапов [12]:

1. Этап фазификации (введение нечеткости). На этом этапе определяются степени истинности для каждого правила:

$A_1(a_0), A_2(a_0), \ldots, A_n(a_0), B_1(b_0), B_2(b_0), \ldots, B_n(b_0)$,

где $A_1(a_0)$ – значение функции принадлежности A_1 переменной a в точке a_0 и т. д.

2. Этап нечеткого вывода:

а) находятся уровни отсечения для предпосылок каждого из правил:

$$\sigma_1 = A_1(a_0) \wedge B_1(b_0),$$
$$\sigma_2 = A_2(a_0) \wedge B_2(b_0),$$
$$\ldots$$
$$\sigma_n = A_n(a_0) \wedge B_n(b_0);$$

в) определяются усеченные функции принадлежности для выходной переменной:

$$C_1' = \sigma_1 \wedge C_1(c),$$
$$C_2' = \sigma_2 \wedge C_2(c),$$
$$\ldots$$
$$C_n' = \sigma_n \wedge C_n(c).$$

3. Этап композиции. Проводится объединение найденных усеченных функций с использованием операции максимума и определяется итоговая функция принадлежности для выходной переменной:

$$\varphi_{\text{итог}}(c) = C(c) = C_1' \vee C_2' \vee \ldots \vee C_n' =$$
$$= C_n'\{\sigma_1 \wedge C_1(c)\} \vee$$
$$\vee\{\sigma_2 \wedge C_2(c)\} \vee \ldots \vee \{\sigma_n \wedge C_n(c)\} =$$
$$= \{A_1(a_0) \wedge B_1(b_0) \wedge C_1(c)\} \vee$$
$$\vee\{A_2(a_0) \wedge B_2(b_0) \wedge C_2(c)\} \vee$$
$$\vee \ldots \vee \{A_n(a_0) \wedge B_n(b_0) \wedge C_n(c)\}.$$

4. Этап дефазификации. Определяется значение выходной переменной c_0 по следующей формуле:

$$c_0 = \frac{\int_0^1 c\varphi_{\text{итог}}(c)dc}{\int_0^1 \varphi_{\text{итог}}(c)dc}.$$

Для получения значений переменной «риск информационной безопасности» по алгоритму нечеткого вывода Мамдани в исследовании использовался пакет Fuzzy Logic Toolbox системы Matlab.

ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

В соответствии с механизмом оценки риска информационной безопасности АСУС необходимо провести формализацию входных переменных.

Для каждой из переменных задается набор термов, например для переменной $a = P_{\text{угр}}$ термножества: «низкая», «средняя», «высокая» и «очень высокая», для переменной $b = C_{\text{ущ}}$ – «малый», «средний», «большой» и «недопустимый», а для переменной $c = Risk$: 1 – «незначительный», 2 – «очень низкий», 3 – «низкий», 4 – «средний», 5 – «высокий», 6 – «недопустимый».

Функции принадлежности термов обозначим следующим образом:

а) вероятность реализации угрозы: $A_1(a)$ – «низкая»; $A_2(a)$ – «средняя»; $A_3(a)$ – «высокая»; $A_4(a)$ – «очень высокая»;

b) ущерб от реализации угрозы: $B_1(b)$ – «малый»; $B_2(b)$ – «средний»; $B_3(b)$ – «большой», $B_4(b)$ – «недопустимый»;

c) риск информационной безопасности: $C_1(c)$ – «незначительный», $C_2(c)$ – «очень низкий», $C_3(c)$ – «низкий», $C_4(c)$ – «средний», $C_5(c)$ – «высокий», $C_6(c)$ – «недопустимый».

Логика связи входных величин (вероятность реализации угрозы и ущерб от реализации угрозы) и риска представлена в таблице 1.

В соответствии с таблицей 1 зададим правила с единичными весовыми коэффициентами, например, если A «низкая» и B «малый», то C

Таблица 1

Логика связи входных величин и риска

Вероятность реализации угрозы	Ущерб от реализации угрозы			
	Малый	Средний	Большой	Недопустимый
Низкая	1	1	2	3
Средняя	1	2	3	4
Высокая	2	3	4	5
Очень высокая	3	4	5	6

«незначительный», если A «низкая» и B «средний», то C «незначительный» и т. д.

На основании опроса экспертов получены следующие субъективные оценки входных переменных:

– вероятность реализации угрозы создания боевым расчетом АСУС нештатных режимов функционирования программных (программно-аппаратных) средств, $a = 0{,}683$;

– ущерб от реализации угрозы, $b = 0{,}741$.

Задача оценки рисков информационной безопасности АСУС различного назначения в работе решена с помощью программного пакета «Matlab». Значение выходной переменной «риск информационной безопасности» получено с использованием алгоритма Мамдани, который заключается в выполнении следующих этапов:

1. Этап фазификации (введение нечеткости). Определим значение функций принадлежности в точках $a = 0{,}683$ и $b = 0{,}741$:

$$\varphi_{A1}(0,683) = 0;\ \varphi_{A2}(0,683) = 0,5;$$
$$\varphi_{A3}(0,683) = 0,3;\ \varphi_{A4}(0,683) = 0;$$
$$\varphi_{B1}(0,741) = 0;\ \varphi_{B2}(0,741) = 0;$$
$$\varphi_{B3}(0,741) = 1;\ \varphi_{B4}(0,741) = 0.$$

2. Этап нечеткого вывода. Степень истинности $A_i(a)$ и $B_i(b)$, а также уровни отсечения $\sigma_i = A_i(a_0) \wedge B_i(b_0)$ для предпосылок каждого из 16 правил представлены в таблице 2.

3. Этап композиции. Итоговая функция принадлежности для выходной переменной получена с использованием операции максимума по объединению найденных усеченных функций:

$$\varphi_{\text{итог}}(c) = C(c) = C_1' \vee C_2' \vee \ldots \vee C_n' =$$
$$= \{\sigma_1 \wedge C_1(c)\} \vee$$
$$\vee\{\sigma_2 \wedge C_2(c)\} \vee \ldots \vee \{\sigma_n \wedge C_n(c)\} =$$
$$= \{A_1(a) \wedge B_1(b) \wedge C_1(c)\} \vee$$
$$\vee\{A_2(a) \wedge B_2(b) \wedge C_2(c)\} \vee$$
$$\vee \ldots \vee \{A_{16}(a) \wedge B_{16}(b) \wedge C_{16}(c)\} =$$
$$= \{0,5 \wedge C_3(c)\} \vee \{0,3 \wedge C_4(c)\}.$$

4. Этап дефазификации. На заключительном этапе алгоритма Мамдани определяется значение выходной переменной (например, как центр тяжести для кривой $\varphi_{\text{итог}}(c)$):

$$c_0 = \frac{\int_0^1 c\phi_{\text{итог}}(c)dc}{\int_0^1 \phi_{\text{итог}}(c)dc} = 0,562.$$

С помощью программного пакета «Matlab» получена графическая интерпретация алгоритма нечеткого вывода Мамдани для рассматриваемого примера (рис. 1).

Кроме того, Fuzzy Logic Toolbox позволяет получить трехмерный график зависимости риска информационной безопасности от вероятности реализации угрозы и ущерба от ее реализации (рис. 2).

График, представленный на рисунке 2, позволяет наглядно оценить адекватность свойств

Таблица 2

Степени истинности для предпосылок каждого правила

Правило №	$A_i(a)$	$B_i(b)$	σ_i
1	0	0	0
2	0	0	0
3	0	1	0
4	0	0	0
5	0	0	0
6	0,5	0	0
7	0,5	1	0,5
8	0,5	0	0
9	0,5	0	0
10	0,3	0	0
11	0,3	1	0,3
12	0,3	0	0
13	0	0	0
14	0	0	0
15	0	1	0
16	0	0	0

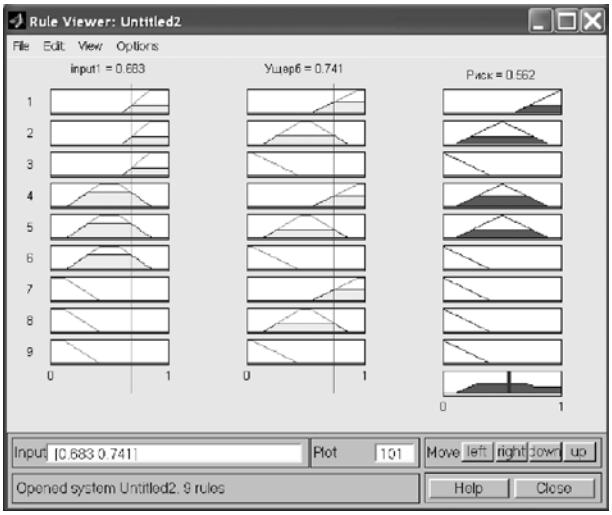

Рис. 1. Графическая интерпретация алгоритма нечеткого вывода Мамдани в Fuzzy Logic Toolbox программного пакета «Matlab»

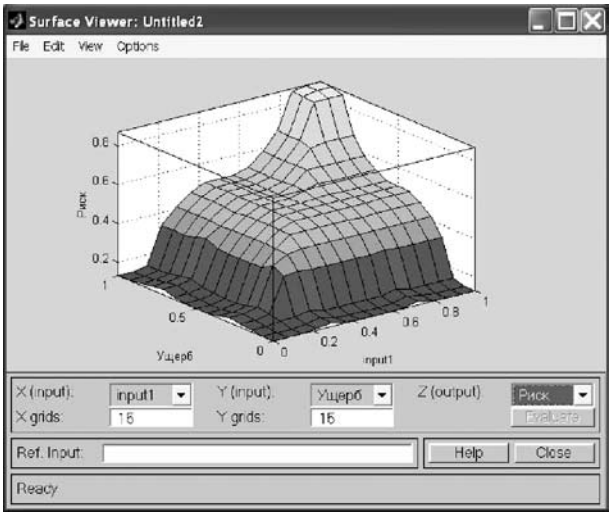

Рис. 2. Зависимость уровня риска информационной безопасности от вероятности реализации угрозы и ущерба

механизма вывода и даже позволяет прогнозировать изменение риска при определенных условиях.

Таким образом, использование алгоритма Мамдани в теории нечетких множеств и нечеткой логики позволит сделать систему управления рисками информационной безопасности АСУС более универсальной, способной описать ситуацию в различных условиях функционирования. Такой подход позволяет заменить приближенные табличные модели грубой оценки рисков современной математической моделью, более адекватной рассматриваемой задаче.

ЗАКЛЮЧЕНИЕ

Использование теории нечетких множеств и нечеткой логики позволит сделать систему управления рисками информационной безопасности АСУС более универсальной, способной описать ситуацию в различных условиях функционирования. Такой подход позволяет заменить приближенные табличные модели грубой оценки рисков современной математической моделью, более адекватной рассматриваемой задаче. Механизм оценивания рисков на основе нечеткой логики по существу является экспертной системой, в которой базу знаний составляют правила, отражающие логику взаимосвязи входных величин и риска.

Предложенный аппарат оценки рисков ИБ позволит оперативно и эффективно решать достаточно широкий класс задач административного управления рисками ИБ АСУС.

Достоинство предложенного подхода состоит в том, что он не требует постановки и решения сложных задач математического программирования. Вместо этого используются экспертные правила «ЕСЛИ – ТО», которые формализуются нечеткой логикой и настраиваются с помощью обучающей выборки.

СПИСОК ЛИТЕРАТУРЫ

1. *Балашов П. А.* Оценка рисков информационной безопасности на основе нечеткой логики / П. А. Балашов, Р. И. Кислов, В. П. Безгузиков // Безопасность компьютерных систем. – 2003. – № 6. – С. 60–65.

2. *Дьяконов В. А.* Математические пакеты расширения MATLAB. Специальный справочник / В. А. Дьяконов, В. С. Круглов. – СПб. : Питер, 2001. – 480 с.

3. *Малюк А. А.* Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк, С. В. Пазизин, М. С. Погожин. – М. : Горячая линия – Телеком, 2001. – 148с.

4. *Остапенко О. А.* Риски систем: оценка и управление / О. А. Остапенко [и др.] ; под ред. Ю. Н. Лаврухина, А. Г. Остапенко. – Воронеж : МИКТ, 2007. – 261 с.

5. *Щербаков В. Б.* Безопасность беспроводных сетей: стандарт IEEE 802.11 / В. Б. Щербаков, С. А. Ермаков. – М. : РадиоСофт, 2010. – 255 с.

6. *Минаев В. А.* Основы информационной безопасности : учебник для высших учебных заведений системы МВД РФ / В. А. Минаев. – Воронеж : Воронежский институт МВД России, 2001. – 464 с.

7. Безопасность информационных технологий. Критерии оценки безопасности информационных

технологий. Руководящий документ. – М. : Гостехкомиссия России, 2002, ч. 1–3.

8. *Дидюк Ю. Е.* Методика выбора комплекса средств защиты информации в автоматизированных системах / Ю. Е. Дидюк // Информация и безопасность. – 2006. – № 2. – С. 45–47.

9. *Петренко С. А.* Управление информационными рисками / С. А. Петренко, С. В. Симонов. – М. : ДМК Пресс, 2004. – 384 с.

10. *Корченко А. Г.* Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко. – Киев : МК – Пресс, 2006. – 320 с.

11. *Глаголев Р. Э.* Разработка алгоритма оценки и управления рисками информационной безопасности на основе метода парных сравнений / Р. Э. Глаголев, С. А. Никулин // IV научные чтения имени А. С. Попова : сб. матер. Всерос. науч.-практ. конф. – Воронеж : ВУНЦ ВВС «ВВА», 2015. – С. 81–83.

12. *Глаголев Р. Э.* Оценка рисков информационной безопасности автоматизированных систем управления и связи на основе теории нечетких множеств и нечеткой логики / Р. Э. Глаголев, С. А. Никулин // Охрана, безопасность, Связь – 2015 : сб. матер. междунар. науч.-практ. конф. – Воронеж : ВИ МВД России, 2015. – С. 113–116.

13. *Кащенко А. Г.* Векторная оценка и минимизация рисков информационной безопасности / А. Г. Кащенко // Информация и безопасность. – 2008. – № 1. – С. 101–104.

14. *Леоненков А. В.* Нечеткое моделирование в среде MATLAB и fuzzyTECH / А. В. Леоненков. – СПб. : БХВ-Петербург, 2003. – 736 с.

TECHNIQUE OF THE QUANTITATIVE ASSESSMENT OF SIZE OF RISK OF ENSURING INFORMATION SECURITY OF AUTOMATED CONTROL SYSTEMS AND COMMUNICATION

© 2016 S. A. Nikulin*, S. S. Nikulin**

** Military training and research center of the air force «Air force academy named after professor N. E. Zhukovsky and Yu. A. Gagarin» (Voronezh), Old Bolsheviks str., 54a, 394064, Voronezh, Russia*
*** Voronezh institute of the Ministry of the Interior of Russia, Patriotov Avenue, 53, 394065, Voronezh, Russia*
E-mail: nikcc@mail.ru

Received 15.01.2016

Annotation. The problem of an assessment of risks of information security of automated control systems and communication (ASUS) on the basis of use of the theory of indistinct sets and fuzzy logic is considered.

In work functions of accessory of indistinct sets with use of an expert method of consecutive intervals are constructed. An example of an assessment of risk of information security from realization of threat of creation by fighting calculation of ASUS of the emergency modes of functioning of program (hardware-software) means with use of algorithm of Mamdani is reviewed.

Keywords: risks of information security, information threat to security, probability of realization of threat, damage from realization of threats, the theory of indistinct sets and fuzzy logic, Mamdani's algorithm.

REFERENCES

1. Balashov P. A., Kislov R. I., Bezguzikov V. P. Otsenka riskov informatsionnoi bezopasnosti na osnove nechetkoi logiki. *Bezopasnost' komp'yuternykh sistem*, 2003, № 6, pp. 60–65.

2. D'yakonov V. A. *Matematicheskie pakety rasshireniya MATLAB. Spetsial'nyi spravochnik*, Saint-Petersburg, Piter, 2001, 480 p.

3. Malyuk A. A., Pazizin S. V., Pogozhin M. S. *Vvedenie v zashchitu informatsii v avtomatizirovannykh sistemakh*, Moscow, Goryachaya liniya – Telekom, 2001, 148 p.

4. Ostapenko O. A. *Riski sistem: otsenka i upravlenie*, Voronezh, MIKT, 2007, 261 p.

5. Shcherbakov V. B. *Bezopasnost' besprovodnykh setei: standart IEEE 802.11*, Moscow, RadioSoft, 2010, 255 p.

6. Minaev V. A. *Osnovy informatsionnoi bezopasnosti: uchebnik dlya vysshikh uchebnykh zavedenii sistemy MVD RF*, Voronezh, Voronezhskii institut MVD Rossii, 2001, 464 p.

7. *Bezopasnost' informatsionnykh tekhnologii. Kriterii otsenki bezopasnosti informatsionnykh*

tekhnologii. Rukovodyashchii document, Moscow, Gostekhkomissiya Rossii, 2002, ch. 1–3.

8. Didyuk Yu. E. Metodika vybora kompleksa sredstv zashchity informatsii v avtomatizirovannykh sistemakh. *Informatsiya i bezopasnost'*, Voronezh, 2006, № 2. pp. 45–47.

9. Petrenko S. A., Simonov S. V. *Upravlenie informatsionnymi*, Moscow, DMK Press, 2004, 384 p.

10. Korchenko A.G. *Postroenie sistem zashchity informatsii na nechetkikh mnozhestvakh. Teoriya i prakticheskie resheniya*, Kiev, MK–Press, 2006, 320 p.

11. Glagolev R. E., Nikulin S. A. *«IV nauchnye chteniya imeni A.S. Popova»*, Proceedings of the All-Russian scientific and practical conference. Voronezh, VUNTs VVS «VVA», 2015. pp. 81–83.

12. Glagolev R.E., Nikulin S.A. *«Okhrana, bezopasnost', svyaz' – 2015»* Proceedings of the international scientific and practical conference. Voronezh, VI MVD Rossii, 2015. pp. 113–116.

13. Kashchenko A. G. Vektornaya otsenka i minimizatsiya riskov informatsionnoi bezopasnosti. *Informatsiya i bezopasnost'*, 2008. № 1, pp. 101–104.

14. Leonenkov A. V. *Nechetkoe modelirovanie v srede MATLAB i fuzzyTECH*, Saint-Petersburg, BKhV-Peterburg, 2003, 736 p.

Никулин Сергей Анатольевич – профессор кафедры организации связи (и технической эксплуатации средств связи) Военного учебно-научного центра военно-воздушных сил «Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина» (г. Воронеж), кандидат физико-математических наук, доцент. E-mail: Nikulin1958@bk.ru

Никулин Сергей Сергеевич – доцент кафедры радиотехники и электроники Воронежского института МВД России, кандидат технических наук. E-mail: nikcc@mail.ru

Nikulin Sergey Anatolyevich – professor of chair of the organization of communication (and technical operation of means of communication) of Military training and research center of the air force «Air force academy named after professor N. E. Zhukovsky and Yu. A. Gagarin», candidate of physical and mathematical sciences, associate professor. E-mail: Nikulin1958@bk.ru

Nikulin Sergey Sergeyevich – associate professor of chair of radio engineering and electronics of Voronezh institute of the Ministry of the Interior of Russia, candidate of technical sciences. E-mail: nikcc@mail.ru