УДК 517.929

© Антонов С.Г., Зорин Э.Ф., Рыжов Б.С., Якименко В.М.
Antonov S., Zorin E., Ryzhov B., Ykimenko V.

ОЦЕНКА ЗАЩИЩЕННОСТИ СРЕДСТВ ИНФОРМАТИЗАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ВОЕННОГО НАЗНАЧЕНИЯ, ФУНКЦИОНИРУЮЩЕЙ В УСЛОВИЯХ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ

ESTIMATION OF SECURITY OF MEANS OF INFORMATION OF THE AUTOMATED MILITARY-ORIENTED SYSTEM, FUNCTIONING IN THE CONDITIONS OF INFORMATIONAL-TECHNICAL ACTIONS

Аннотация. *В статье рассматривается оценка защищенности средств информатизации автоматизированной системы военного назначения (АС ВН), функционирующей в условиях информационно-технических воздействий (ИТВ), экспериментально-аналитическим способом с использованием инструментальных средств сканирования испытуемых систем и последующей аналитической обработкой результатов на основе метода анализа иерархий. Приведены основные аналитические соотношения оценки защищенности средств информатизации АС ВН, функционирующих в условиях ИТВ, полученные на основе «транзитивных шкал» метода Т.Саати. Дана оценка эффективности предложенного способа оценки защищенности средств информатизации АС ВН, функционирующих в условиях ИТВ.*

Annotation. *In paper the estimation of security of means of information of the automated military-oriented system (AS MO), functioning in the conditions of informational-technical actions (ITA) by an experimentally-analytical method with usage of work benches of scanning of examinees of systems and the subsequent analytical handling of outcomes on the basis of a method of the analysis of hierarchies is considered. The main analytical ratios of an estimation of security of means of information AS MO, functioning in the conditions of ITA, received on a basis of «transitive dials» T.Saati's method are reduced. The estimation of efficiency of the offered method of an estimation of security of means of information AS MO, functioning in the conditions of ITA is given.*

Ключевые слова. *Автоматизированная система, оценка защищенности, коэффициенты весомости.*

Key words. *The automated system, estimation to zaschischennosti, factor weights.*

Решение задачи оценки защищенности АС ВН, функционирующих в условиях ИТВ, предполагает экспериментальное определение уязвимости средств автоматизации АС ВН, проведение их классификации и ранжирования по уровням уязвимости путем расчёта коэффициентов весомости и определение комплексного показателя защищенности средств автоматизации АС ВН.

Эффективность функционирования средств автоматизации АС ВН во многом определяется их защищенностью при выполнении ими функций сбора, обработки, представления данных и передачи информации.

Возможность реализации на средства информатизации АС ВН широкого спектра ИТВ диктует необходимость проведения системных исследований, направленных на разработку адекватных способов оценки защищенности средств информатизации АС ВН, функционирующих в условиях различных деструктивных ИТВ, и создания на их основе средств обеспечения информационной безопасности.

В такой постановке задача сводится к определению количественных оценок функциональных характеристик средств информатизации АС ВН в зависимости от

Антонов Сергей Григорьевич – начальник отдела, 4 ЦНИИ Минобороны России, тел. (495) 515-25-75;
Зорин Эдуард Фёдорович – кандидат технических наук, старший научный сотрудник, ведущий научный сотрудник, 4 ЦНИИ Минобороны России;
Рыжов Борис Сергеевич – кандидат технических наук, старший научный сотрудник, 4 ЦНИИ Минобороны России;
Якименко Владимир Михайлович – научный сотрудник, 4 ЦНИИ Минобороны России.

Antonov Sergey – the chief of department, 4 Central Scientific Research Institute Ministry of Defence of Russia, tel. (495) 515-64-28;
Zorin Eduard – Cnd.Sci.Tech., the senior scientific employee, the senior scientific employee, 4 CSRI Ministry of Defence of Russia.
Ryzhov Boris – Cnd.Sci.Tech., high scientific employee, 4 CSRI Ministry of Defence of Russia;
Ykimenko Vladimir –scientific employee, 4 CSRI Ministry of Defence of Russia.

применяемых в них средств защиты информации и других факторов, оказывающих влияние на дисциплину их функционирования.

Использование в средствах информатизации АС ВН стандартных средств защиты информации, таких как межсетевые экраны и антивирусные программы, не гарантируют адекватности реальной защиты средств информатизации АС ВН, функционирующих в условиях ИТВ, требованиям по обеспечению безопасности информации [1] в силу специфических особенностей средств информатизации АС ВН. К числу таких особенностей относятся:

• высокий уровень территориальной распределенности объектов АС ВН;

• большое разнообразие применяемых информационных технологий;

• возможность перехвата данных в магистральных сетях, возрастающая при их переводе на зарубежное телекоммуникационное оборудование;

• высокий уровень риска быть подверженным ИТВ вследствие применения в АС ВН коммерческих программных средств, в том числе нелицензионного и несертифицированного программного оборудования;

• отсутствие документированных данных сценариев, форм и способов ИТВ, являющихся исходными данными для решения задач эффективного противодействия.

Несовершенство средств защиты информации АС ВН приводит к тому, что в реальных условиях неизвестные ИТВ, преодолевая рубежи защиты в средствах информатизации АС ВН, оказывают деструктивные воздействия на эффективность функционирования АС ВН.

Исходя из изложенного, оценка защищенности средств информатизации АС ВН, функционирующих в условиях деструктивных ИТВ, представляет собой достаточно сложную многокритериальную задачу с иерархической структурой. В силу этого решение такой задачи целесообразно осуществлять с использованием метода анализа иерархий [3], позволяющего включать в оценку свойств АС ВН наиболее полный объем знаний о характеристиках средств информатизации АС ВН.

Метод анализа иерархий объединяет в себе аналитический подход, опирающийся на теорию матриц с экспертными процедурами. Метод является замкнутой логической конструкцией, обеспечивающей анализ специфических свойств оцениваемых средств информатизации во всем их многообразии с помощью простых правил и приводящей, в конечном итоге, к наилучшему результату.

Для оценки защищенности средств информатизации АС ВН предлагается применять экспериментально-аналитический способ, предполагающий использование программно-инструментальных средств сканирования оцениваемых систем с последующей аналитической обработкой полученных результатов на основе «транзитивных шкал» метода анализа иерархий. К программно-инструментальным средствам сканирования относятся, в частности, средства систем обнаружения компьютерных атак, СОА-1, XSpider и другие.

Таким образом, задача оценки защищенности средств информатизации АС ВН, функционирующих в условиях ИТВ, может быть сформулирована следующим образом.

Задано множество характеристик сканирования средств информатизации АС ВН $q_i^*, i = \overline{1,6}$ программно-аппаратными средствами систем обнаружения компьютерных атак.

Такими характеристиками являются: критически важные информационные объекты испытуемых систем, перечень уязвимостей, их количество, степень опасности и другие характеристики сканирования АС ВН. Важно отметить, что результаты сканирования представляют собой весьма разнородные характеристики по уровням уязвимости, их количеству и степени опасности.

Необходимо оценить реальный уровень защищенности средств информатизации АС ВН, функционирующих в условиях ИТВ, на основе анализа их тактико-технических характеристик и результатов сканирования.

Решение поставленной задачи осуществляется в три последовательных этапа.

На первом этапе проводится анализ характеристик результатов сканирования q_i^* и степень опасности их реализации.

Перечень характеристик, полученных в процессе сканирования средств информатизации и степени опасности их реализации, приведен в табл.1.

Таблица 1

Характеристики опасности реализации уязвимостей

Степень опасности реализации уязвимостей	Количественное значение характеристик уязвимостей (q_i^*)
Высокий уровень опасности	13
Подозрение на высокий уровень опасности	50
Средний уровень опасности	88
Подозрение на средний уровень опасности	51
Низкий уровень опасности	127
Опасности нет	0

Далее производится приведение характеристик q_i^* к единой оценочной шкале путем их нормализации

по формуле

$$q_i = q_i^* / \sum_{i=1}^{6} q_i^*; \quad i = \overline{1,6}. \qquad (1)$$

На втором этапе определяются показатели уязвимости средств информатизации из соотношения

$$Q_{\text{уязi}} = w_i q_i; \quad i = \overline{1,6}. \qquad (2)$$

При определении показателей $Q_{\text{уязi}}$ возникает необходимость определения коэффициентов весомости w_i, определяющих относительную важность оцениваемых средств с точки зрения из уязвимости. Процесс определения коэффициентов весомости предполагает формирование матрицы попарных сравнений характеристик уязвимости оцениваемых средств информатизации АС ВН. В общем случае матрица попарных сравнений А представляет собой обратносимметричную матрицу [2] размерности 6×6 вида

$$\mathbf{A} = \begin{Vmatrix} 1 & a_{12} & a_{13} & \dots & a_{16} \\ a_{21} & 1 & a_{23} & \dots & a_{26} \\ \dots & \dots & \dots & \dots & \dots \\ a_{61} & a_{62} & a_{63} & \dots & 1 \end{Vmatrix}, \qquad (3)$$

в которой элементы $a_{ij}; \quad i, j = \overline{1,6}$ над главной диагональю коэффициенты превосходства i-го свойства (характеристики) над *j*-м свойством (характеристикой) выбираются согласно балльной шкалы соотношений [3]

$$\{1/9, 1/8, 1/7, 1/6, 1/5, 1/4, 1/3, 1/2, 1, 2, 3, 4, 5, 6, 7, 8, 9\}. \qquad (4)$$

При этом численные значения шкалы имеют следующую интерпретацию:

1 – характеристики оцениваемых средств имеют одинаковую важность;

3 – одна характеристика несколько важнее другой;

5 – одна характеристика важнее другой;

7 – одна характеристика имеет существенное превосходство над другой;

9 – одна характеристика имеет абсолютное превосходство над другой.

Примечание: Значения степеней превосходства 2, 4, 6, 8 имеют промежуточные интерпретации.

Следует отметить, классический метод Т. Саати в целом обеспечивает приемлемую точность оценки защищенности испытываемых средств информатизации АС ВН, однако обладает достаточно большой сложностью в силу трудоемкости определения собственных значений матричного уравнения $\mathbf{A} \cdot \mathbf{w} = \lambda_{\max} \cdot \mathbf{w}$.

С целью снижения трудоемкости вычислительного процесса предлагается для формирования матрицы А попарных сравнений использовать «транзитивные» шкалы [4] типа:

слабое превосходство – a;
сильное превосходство – a^2;
очень сильное превосходство – a^3,
абсолютное превосходство – a^4. (5)

В этом случае для определения коэффициентов весомости достаточно иметь цепочку коэффициентов превосходства вида $a_{12}, a_{23},..., a_{56}$, являющихся элементами матрицы А и находящихся над её главной диагональю. При формировании элементов матрицы А могут быть приняты [4] значения базовых коэффициентов, равными a=1,5 или a=2. С учётом изложенного коэффициенты превосходства будут иметь значения, представленные в табл. 2.

Таким образом, элементы матрицы попарных сравнений $a_{i1}, a_{i2},..., a_{i6}$ есть не что иное, как отношения

Таблица 2

Коэффициенты превосходства

Смысловая интерпретация	$a = 1{,}5$	$a = 2$
Слабое превосходство	1,5	2
Сильное превосходство	2,25	4
Очень сильное превосходство	3,38	8
Абсолютное превосходство	5,06 и более	16 и более

$$\frac{w_i}{w_1}, \frac{w_i}{w_2}, .., \frac{w_i}{w_6}.$$

При этом элемент матрицы $a_{ij} = w_i / w_j$ получается на основе попарного сравнения элементов *i* и *j*-го друг с другом по общему для них свойству (характеристике). Элемент *i*, в меньшей степени обладающий этим свойством, принимается равным единице, а элемент *j* представляется числом, кратным этой единице. Отношение $a_{ij} = w_i / w_j$, при a=1,5 означает, что элемент *i*-й имеет слабое превосходство над элементом *j*. Условие $a_{ij} = w_i / w_j$, при a=2,25 означает, что элемент *i*-й имеет сильное превосходство над элементом *j* и т.д. Как следует из работы [2], матрица попарных сравнений А с наддиагональными элементами $a_{12}, a_{23}, ..., a_{56}$ является достаточной для определения коэффициентов весомости.

При этом справедливы соотношения

$$w_1 = 1; \; w_2 = w_1 / a_{12}; \; w_3 = w_1 / a_{12}a_{23};$$
$$w_4 = w_1 / a_{12}a_{23}a_{34}; \; w_5 = w_1 / a_{12}a_{23}a_{34}a_{45}; \qquad (6)$$
$$w_6 = w_1 / a_{12}a_{23}a_{34}a_{45}a_{56}.$$

При этом условие нормирования вектора $w_i, \quad i = \overline{1,6}$ определяется из соотношения

$$\sum_{i=1}^{6} w_i = w_1(1 + w_1 / a_{12} + $$
$$+ w_1 / a_{12}a_{23} + \dots + w_1 / a_{12}a_{23}a_{34}a_{45}a_{56}) = 1. \qquad (7)$$

С учетом изложенного нормированные значения коэффициентов весомости $w_i^{\text{н}}, \quad i=\overline{1,6}$ будут иметь вид

$$w_1^{\text{н}}=\frac{1}{1+w_1/a_{12}+w_1/a_{12}a_{23}+\ldots+w_1/a_{12}a_{23}a_{34}a_{45}a_{56}};$$

$$w_2^{\text{н}}=\frac{w_1^{\text{н}}}{a_{12}};\ w_3^{\text{н}}=\frac{w_1^{\text{н}}}{a_{12}a_{23}};\ w_4^{\text{н}}=\frac{w_1^{\text{н}}}{a_{12}a_{23}a_{34}};\qquad (8)$$

$$w_5^{\text{н}}=\frac{w_1^{\text{н}}}{a_{12}a_{23}a_{34}a_{45}};\ w_6^{\text{н}}=\frac{w_1^{\text{н}}}{a_{12}a_{23}a_{34}a_{45}a_{56}}.$$

Коэффициенты превосходства $a_{ij}; \quad i,j=\overline{1,6}$ соотношений (8) выбираются оператором в соответствии с балльной шкалой табл. 2.

На третьем этапе рассчитывается комплексный показатель уязвимости средств информатизации АС ВН по зависимости

$$Q_{\text{уяз}}=\sum_{i=1}^{6}w_i^{\text{н}}q_i, \qquad (9)$$

где $w_i^{\text{н}}, \quad i=\overline{1,6}$ – нормированные значения коэффициентов весомости опасности уязвимостей средств информатизации АС ВН;

$q_i, i=\overline{1,6}$ – нормированные значения характеристик сканирования средств информатизации АС ВН.

По полученным значениям показателя уязвимости $Q_{\text{уяз}}$ средств информатизации АС ВН определяется комплексный показатель их защищенности $P_{\text{защ}}$ из соотношения

$$P_{\text{защ}}=1-Q_{\text{уяз}}, \qquad (10)$$

представляющий собой средневзвешенную величину способности средств защиты информатизации АС ВН обеспечивать её безопасность в случае ИТВ.

В качестве примера для характеристик $q_i^*, \quad i=\overline{1,6}$ результатов сканирования средств информатизации АС ВН, представленных в табл. 1, в соответствии с изложенной методикой определены количественные значения коэффициентов весомости $w_i^{\text{н}}, \quad i=\overline{1,6}$

$$w_1^{\text{н}}=0,37; \quad w_2^{\text{н}}=0,24; \quad w_3^{\text{н}}=0,16;$$
$$w_4^{\text{н}}=0,11, \quad w_5^{\text{н}}=0,07, \quad w_6^{\text{н}}=0,05.$$

С учетом полученных результатов значение показателя уязвимости средств информатизации АС ВН, рассчитанное по формуле (9), составляет $Q_{\text{уяз}}=0,137$.

При этом значение комплексного показателя защищенности средств информатизации АС ВН в соответствии с соотношением (10) будет равно $P_{\text{защ}}=0,863$.

В соответствии с требованиями руководящих и нормативно-методических документов в области информационной безопасности допустимые значения комплексного показателя защищенности средств информатизации АС ВН при повышенном и допустимом рисках характеризуются значениями, представленными в табл. 3.

Таблица 3

Допустимые значения показателя защищенности средств информатизации АС ВН

Показатели защищенности	Допустимые значения показателей защищенности $P_{\text{защ}}^{\text{доп}}$	
	при повышенном риске	при допустимом риске
Комплексный показатель защищенности средств информатизации АС ВН от возможных деструктивных ИТВ	0,90	0,95

Полученное значение комплексного показателя указывает на необходимость проведения дополнительных мероприятий по повышению уровня защищенности испытуемых средств информатизации АС ВН.

Выводы

Из изложенного следует:

1. Оценка защищенности средств информатизации АС ВН, функционирующих в условиях ИТВ, является сложной многокритериальной задачей с иерархической структурой.

Решение такой задачи представляется обоснованным осуществлять на основе метода анализа иерархий, объединяющего в себе:

• результаты уязвимостей средств информатизации АС ВН, полученные экспериментально с помощью программно-аппаратных средств систем обнаружения ИТВ;

• аналитические методы определения коэффициентов весомости, необходимые для расчета комплексных показателей уязвимости и защищенности средств информатизации АС ВН.

2. Использование в задаче оценки защищенности средств информатизации АС ВН экспериментально-аналитического способа выявления уязвимостей с помощью сканеров, в сочетании с экспертными процедурами определения важности уязвимостей средств информатизации АС ВН на основе «транзитивных» шкал метода анализа иерархий, обеспечивает приемлемый уровень достоверности получаемых оценок защищенности АС ВН, функционирующих в условиях ИТВ при существенном снижении трудоемкости вычислительного процесса.

3. В условиях некоторой неопределенности состава и характеристик выявленных уязвимостей предложенный способ оценки защищенности средств информатизации АС ВН, функционирующих в условиях ИТВ, являет-

ся эффективным механизмом снижения риска принятия неадекватных решений по защите информационных ресурсов АС ВН.

4.Следует иметь в виду, что использование упрощенного метода формирования матрицы попарных сравнений в отдельных случаях может приводить к достаточно приближенным оценкам. В этом случае необходимо переходить к уточнению процедуры формирования матрицы попарных сравнений.

Литература

1. Мельников В.В. Безопасность информации в автоматизированных системах. - М: Финансы и статистика, 2003 – 368 с.
2. Беллман Р. Введение в теорию матриц. – М.: НАУКА, 1976. – 351 с.
3. Саати Т. Принятие решений. Метод анализа иерархий: Пер. с англ. - М.: Радио и связь. 2006. – 320 с.
4. Черноруцкий И.Г. Методы принятия решений. - Спб.: БХВ-Петербург, 2005. – 416 с.
5. Молчанов А.А. Моделирование и проектирование сложных систем. Киев. Высшая школа. Головное изд-во. 1988. – 359 с.
6. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008. – 544 с.

Материал поступил в редакцию 16. 02. 2012 г.