УДК 004.65 Вестник УрФО № 1(55) / 2025, с. 37–44

Сенцова А. Ю., Арсланова Г. И., Русинова Д. С. DOI: 10.14529/secur250104

МЕТОД МНОГОКРИТЕРИАЛЬНОГО ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Данная статья посвящена решению актуальной проблемы выбора средств защиты информации (СрЗИ) в условиях роста количества угроз и расширения доступных на рынке решений. Авторами предлагается метод многокритериального выбора средств защиты информации, основанный на методике комплексной оценки структур. Метод включает девять основных этапов, от определения множества альтернатив до выбора наиболее рационального средства защиты. В рамках подхода учитываются как субъективные предпочтения экспертов и заказчиков, так и объективные технические характеристики средств защиты, включая их совместимость и функциональность. Приведен пример практического применения метода на примере выбора антивирусных программ, что подчеркивает универсальность предложенного подхода. Дальнейшее развитие метода направлено на его автоматизацию, что позволит снизить трудозатраты и повысить точность выбора оптимальных решений.

Ключевые слова: *информационная безопасность, многокритериальный, система защиты, поиск оптимального выбора, угрозы, информационные риски.*

Sentsova A. U., Arslanova G. I., Rusinova D. S.

THE METHOD OF MULTI-CRITERIA SELECTION OF INFORMATION SECURITY TOOLS

This article is devoted to solving the urgent problem of selecting information protection equipment (IPE) in the context of the growing number of threats and the expansion of solutions available on the market. The authors propose a method of multi-criteria selection of information protection means based on the technique of complex evaluation of structures. The method includes nine main stages, from the definition of a set of alternatives to the selection of the most rational means of protection. The approach takes into account both subjective preferences of experts and customers and objective technical characteristics of protection means, including their compatibility and functionality. An example of practical application of the method is given on the example of selecting anti-virus programmes, which emphasises the universality of the proposed approach. Further development of the method is aimed at its automation, which will reduce labour costs and increase the accuracy of selecting optimal solutions.

Keywords: *information security, multi-criteria, protection system, search for optimal choice, threats, information risks.*

Введение

На сегодняшний день проблема выбора средств защиты информации (СрЗИ) при планировании специалистом по информационной безопасности (ИБ) модульного состава СрЗИ становится все более актуальной и насущной в связи с расширением предложений и количества возможных альтернатив СрЗИ на рынке. Вместе с тем, при выборе СрЗИ специалист обязан не только руководствоваться нормативной правовой базой в области ИБ и функциональными возможностями тех или иных средств защиты, но и учитывать особенности объекта защиты, предпочтения владельца объекта защиты и возможность совместимости различных средств защиты между собой. Кроме того, для выбора средства защиты из множества альтернатив необходимо использовать метод, который учитывал бы не только субъективное мнение эксперта, но и объективные критерии выбора СрЗИ, которые представляют собой технические характеристики средства защиты, параметры совместимости, реализованные функции и независимые экспертные оценки, статистические данные по каждой из альтернатив.

Таким образом, для решения проблемы выбора СрЗИ специалисту необходим аналитический метод, позволяющий осуществить многокритериальный выбор между возможными альтернативами, предложенными современными поставщиками средств защиты информации, который учитывал бы все вышеперечисленные требования.

В статье предложен метод многокритериального выбора средств защиты информации, основанный на методике комплексной оценки структур описанный в [1]. Метод, предложенный в работе, учитывает критерии выбора различных альтернатив средств защиты, степень важности критерия для владельца объекта защиты, а также меру разумной точности измерения соответствующего критерия для объекта защиты.

Метод многокритериального выбора средств защиты информации базируется на методологии системного анализа и представляет собой пошаговый процесс, первым этапом которого является выбор возможных альтернатив СрЗИ, которые соответствуют классу автоматизированной информационной системы [2] или ее уровню защищенности [3] в соответствии с нормативными правовыми документами в области защиты информации [4], а последним этапом определение наиболее рациональной альтернативы для проектирования или модернизации системы защиты информации.

Для решения проблемы выбора средств защиты информации с помощью метода многокритериального выбора в работе выделено девять основных этапов:

1. определение множества альтернатив СрЗИ, исходя из оценки существующей системы защиты информации объекта защиты;

2. выявление специалистом множества (совокупности) частных критериев, характеризующих альтернативы СрЗИ;

3. построение матрицы критериев альтернатив СрЗИ;

4. составление матрицы бинарных предпочтений, которая содержит результаты попарных сравнений критериев средства защиты по важности;

5. вычисление весов частных критериев исходя из разброса векторных оценок, а также нахождение усредненных весов частных критериев, с учетом предпочтений заказчика, мнения эксперта и аналитических расчетов;

6. перевод векторных оценок СрЗИ в безразмерную величину с помощью значения кванты;

7. построение матрицы векторных оценок, отображающих в табличной форме критерии СрЗИ и направление их экстремума;

8. свертка векторных оценок в обобщенные скалярные оценки;

9. выбор наилучшей альтернативы на основе аналитических расчетов обобщенных скалярных оценок.

Для успешной модернизации существующей системы защиты информации необходимо тщательно изучить политику безопасности предприятия, определить и категорировать основные активы, выделить угрозы безопасности и уязвимости объекта защиты, построить модель угроз и посчитать риски нарушения информационной безопасности. После анализа уровня риска и основных уязвимостей компонентов инфраструктуры, принимается решение модернизировать существующую систему защиты информации и определяется множество альтернатив средств защиты информации, которые будут либо новым барьером на пути распространения угрозы, либо заменят другое средство защиты, уязвимость которого признана экспертами наиболее существенной.

Таблица 1

Матрица критериев альтернатив средств защиты информации

K_i / S_j	S_1	S_2	…	S_{n-1}	S_n	Направление экстремума
K_1	P_{11}	*P12*	…	$P_{1,n-1}$	P_{1n}	min/max
K_2	P_{21}	*P22*	…	$P_{2,n-1}$	P_{2n}	min/max
…	…	…	…	…	…	min/max
K_{m-1}	$P_{m-1,1}$	*Pm-1,2*	…	$P_{m-1,n-1}$	$P_{m-1,n}$	min/max
K_m	P_{m1}	*Pm2*	…	$P_{m,n-1}$	P_{mn}	min/max

Разработка многокритериального метода выбора средств защиты

Для выбора СрЗИ из множества альтернатив, специалист по защите информации должен выявить частные критерии, которые будут характеризовать каждую рассматриваемую в процессе выбора альтернативу. Выявление частных критериев выбора СрЗИ является творческой неформализуемой задачей, которая выполняется специалистом по защите информации на основе его знаний, опыта и характеристик, декларируемых производителем СрЗИ [5]. Для выявления таких критериев специалистом могут быть использованы любые инструменты для получения знаний об альтернативе: аналитические, статистические, имитационные и т.д. На основе полученных экспертом данных формируется множество частных критериев.

1. На начальном этапе для выбора СрЗИ специалисту в области ИБ нужно определить совокупность альтернатив, удовлетворяющих целевую функцию области исследования и совокупность частных критериев для оценки качественных и количественных характеристик СрЗИ.

2. На основе совокупности критериев $\{K_m\}$ и альтернатив СрЗИ $\{S_n\}$ строится матрица (Таблица 1) и выполняется количественная оценка (P_{ij}) СрЗИ по каждому критерию.

3. На следующем этапе составляется бинарная матрица предпочтений {Ki} (Таблица 2). Каждая ячейка в матрице – это результат попарного сравнения частных критериев по важности. 1 – если критерий строки важнее чем критерий столбца. 0,5 – если они равны. 0 – если важность критерия столбца выше, чем важность критерия строки.

Дополнительный столбец C_i – это общая оценка важности критерия, которая вычисляется по формуле 1:

$$C_i = \sum_{j=1}^{m} K_{ij}, \qquad (1)$$

Таблица 2

Бинарная матрица предпочтений

K_i	K_1	K_2	…	K_{m-1}	K_m	C_i
K_1	–	$K_1 \perp K_2$	…	$K_1 \perp K_{m-1}$	$K_1 \perp K_m$	$\sum_{j=1}^{m}(K_1 \perp K_j)$
K_2	$K_2 \perp K_1$	–	…	$K_2 \perp K_{m-1}$	$K_2 \perp K_m$	$\sum_{j=1}^{m}(K_2 \perp K_j)$
…	…	…	–	…	…	…
K_{m-1}	$K_{m-1} \perp K_1$	$K_{m-1} \perp K_2$	…	–	$K_{m-1} \perp K_m$	$\sum_{j=1}^{m}(K_{m-1} \perp K_j)$
K_m	$K_m \perp K_1$	$K_m \perp K_2$	…	$K_m \perp K_{m-1}$	–	$\sum_{j=1}^{m}(K_m \perp K_j)$

4. Следующим шагом эксперта станет вычисление весов частных критериев (Таблица 3), отражающих его предпочтение, исходя из разброса векторных оценок:

$$S_i^{\wedge} = \frac{1}{n} \times \sum_{j=1}^{n} S_{ij}, \quad (2)$$

$$\partial_{1i} = \frac{C_i}{\sum_{i=1}^{m} C_i}, \quad (3)$$

$$r_i = \frac{1}{n} \times \sum_{j=1}^{n} \frac{\left|S_{ij} - S_i^{\wedge}\right|}{S_i^{\wedge}}, \quad (4)$$

$$\partial_{2i} = \frac{r_i}{\sum_{i=1}^{m} r_i}. \quad (5)$$

5. Вычисляем усредненные веса частных критериев Ω_i, i=1, …, m.

$$\Omega_i = \alpha \times \partial_{1i} + \beta \times \partial_{2i}. \quad (6)$$

Коэффициенты α и β характеризуют степень доверия к весам, их сумма всегда равна 1.

6. На следующем этапе необходимо построить матрицу безразмерных оценок. Данная матрица включает в себя сведения из матрицы совокупности критериев и альтернатив и переменную ΔK. Переменная ΔK_i – это величина шага для частного критерия, при котором лицо, принимающее решение (ЛПР), реагирует на изменение значения критерия. Например, при подсчете скорости передачи информации в современном мире величина равная 1 Кб в большинстве случаев является неощутимой, незначительной для организации бизнес-процессов, а 10 Мбит напротив, может вызвать проблемы для реализации бизнес-процессов и может быть зафиксировано ЛПР. Также, эту величину можно считать мерой разумной точности измерения характеристики, то есть степенью приближения результатов расчетов по предлагаемому многокритериальному методу к некоторому действительному значению, которое необходимо учитывать при построении либо модернизации системы защиты информации на предприятии принимая во внимание предпочтения руководителя предприятия, построенную модель угроз (адаптированный базовый набор средств защиты) и требования нормативной правовой базы в области информационной безопасности.

В таблице 4 представлена матрица безразмерных оценок в общем виде. Столбец «Единицы измерения» заполняется в том случае, если у конкретного критерия можно выделить единицу измерения. Также, в случае такого критерия как «стоимость средства защиты информации», в данном столбце указывается, какое количество лицензий включает в себя данный критерий. Рекомендуется привести количество лицензий для конкретного средства защиты к единому значению.

7. Для приведения матрицы от безразмерной оценки к взвешенной оценке, необходимо значения СрЗИ по каждому критерию разделить на соответствующую величину кванты. Кванта рассчитывается по формуле 7:

$$P_{ij}^{new} = \frac{P_{ij}^{old}}{\Delta K_i}. \quad (7)$$

Таблица 3

Таблица весов частных критериев

K_i	$S_i^{\wedge}$	∂_{1i}	r_i	∂_{2i}
K_1	$\frac{1}{n} \times \sum_{j=1}^{n} S_{1j}$	$\frac{C_i}{\sum_{i=1}^{m} C_i}$	$\frac{1}{n} \times \sum_{j=1}^{n} \left\|S_{1j} - S_1^{\wedge}\right\|$	$\frac{r_1}{\sum_{i=1}^{m} r_i}$
K_2	$\frac{1}{n} \times \sum_{j=1}^{n} S_{2j}$	$\frac{C_i}{\sum_{i=1}^{m} C_i}$	$\frac{1}{n} \times \sum_{j=1}^{n} \left\|S_{2j} - S_2^{\wedge}\right\|$	$\frac{r_2}{\sum_{i=1}^{m} r_i}$
…	…	…	…	…
K_{m-1}	$\frac{1}{n} \times \sum_{j=1}^{n} S_{m-1j}$	$\frac{C_i}{\sum_{i=1}^{m} C_i}$	$\frac{1}{n} \times \sum_{j=1}^{n} \left\|S_{m-1j} - S_{m-1}^{\wedge}\right\|$	$\frac{r_{m-1}}{\sum_{i=1}^{m} r_i}$
K_m	$\frac{1}{n} \times \sum_{j=1}^{n} S_{mj}$	$\frac{C_i}{\sum_{i=1}^{m} C_i}$	$\frac{1}{n} \times \sum_{j=1}^{n} \left\|S_{mj} - S_m^{\wedge}\right\|$	$\frac{r_m}{\sum_{i=1}^{m} r_i}$

Таблица 4

Матрица безразмерных оценок

K_i	ΔK_i	Единицы измерения	S_1	S_2	…	$Sn\text{-}1$	Sn
K_1	ΔK_1		P_{11}	P_{12}	…	$P_{1n\text{-}1}$	P_{1n}
K_2	ΔK_2		P_{21}	P_{22}	…	$P_{2n\text{-}1}$	P_{2n}
…	…		…	…	…	…	…
$K_{m\text{-}1}$	$\Delta K_{m\text{-}1}$		$P_{m\text{-}11}$	$P_{m\text{-}12}$	…	$P_{m\text{-}1n\text{-}1}$	$P_{m\text{-}1n}$
K_m	ΔK_m		P_{m1}	P_{m2}	…	$P_{mn\text{-}1}$	P_{mn}

8. На данном этапе необходимо получить оценки мер эффективности (E) для каждой альтернативы по каждой характеристике при помощи обобщенных весов критериев как это показано на формуле 8:

$$E_{ij} = P_{ij} \times \Omega_i. \quad (8)$$

9. На заключительном этапе для нахождения наиболее рационального СрЗИ необходимо найти обобщенные скалярные оценки, путем нахождения разницы между суммарно взвешенными оценками со стороны минимизации и максимизации, по формуле 9:

$$Q_j = \sum_{e=max} S_{ej} - \sum_{e=min} S_{ej}. \quad (9)$$

Пример расчета выбора рационального варианта СрЗИ

Определимся с совокупностью альтернатив $\{S_i\}$ СрЗИ, рассматриваются антивирусные системы:

- Антивирус Dr.Web
- Kaspersky Antivirus
- ESET NOD32 антивирус

Критерии $\{K_i\}$ характерные для антивирусных систем:

- Стоимость [руб.]
- Необходимая минимальная частота процессора [ГГц]
- Необходимое минимальное количество ОЗУ [Мб]

Ниже в таблицах приведены результаты поэтапных вычислений.

Таблица 5

Матрица оценок эффективности

K_i	Ω_i	Единицы измерения	Направление экстремума (e)	S_1	S_2	…	$S_{n\text{-}1}$	S_n
K_1	Ω_1		min/max	E_{11}	E_{12}	…	$E_{1n\text{-}1}$	E_{1n}
K_2	Ω_2		min/max	E_{21}	E_{22}	…	$E_{2n\text{-}1}$	E_{2n}
…	…		min/max	…	…	…	…	…
$K_{m\text{-}1}$	$\Omega_{m\text{-}1}$		min/max	$E_{m\text{-}11}$	$E_{m\text{-}12}$	…	$E_{m\text{-}1n\text{-}1}$	$E_{m\text{-}1n}$
K_m	Ω_m		min/max	E_{m1}	E_{m2}	…	$E_{mn\text{-}1}$	E_{mn}

Таблица 6

Матрица критериев альтернатив средств защиты информации

K_i / S_j	S_1	S_2	S_3	Единицы измерения	Направление экстремума
K_1	1090	1320	990	Руб.	min
K_2	1,5	1	1,3	Ггц	min
K_3	512	2048	1024	Мб	min

Таблица 7

Бинарная матрица предпочтений

K_i	K_1	K_2	K_3	C_i
K_1		1	1	2
K_2	0		0,5	0,5
K_3	0	0,5		0,5

Таблица 8

Таблица весов частных критериев

K_i	S_i^	∂_{1i}	r_i	∂_{2i}
K_1	1133,3	0,6	0,109	0,151
K_2	1,26	0,16	0,14	0,193
K_3	1194.6	0,16	0,476	0,655

$$S_1^{\wedge} = \frac{1090+1320+990}{3} = 1133{,}3,$$

$$\partial_{11} = \frac{2}{2+0{,}5+0{,}5} \approx 0{,}6,$$

$$r_1 = \frac{1}{3} \times \left(\frac{|1090-1133{,}3|}{1133{,}3} + \frac{|1320-1133{,}3|}{1133{,}3} + \frac{|990-1133{,}3|}{1133{,}3} \right) = 0{,}109,$$

$$\partial_{21} = \frac{0{,}109}{0{,}109+0{,}140+0{,}476} = 0{,}151$$

Таблица 9

Матрица безразмерных оценок

K_i	ΔK_i	Единицы измерения	S_1	S_2	S_3
K_1	100	Руб	10,9	13,2	9,9
K_2	0,1	Ггц	15	10	13
K_3	100	Мб	5,12	20,48	10,24

$$P_{11}^{new} = \frac{1090}{100} = 10{,}9$$

Таблица 10

Матрица оценок мер эффективности

K_i	Ωi	Единицы измерения	Направление экстремума (e)	S_1	S_2	S_n
K_1	0,3755	Руб.	min	4,092	4,956	3,717
K_2	0,1765	Ггц	min	2,647	1,765	2,294
K_3	0,4075	Мб	min	2,086	8,345	4,172

$$\Omega_1 = 0{,}6 \times 0{,}5 + 0{,}151 \times 0{,}5 = 0{,}3755$$

$$E_{11} = 10{,}9 \times 0{,}3755 = 4{,}092$$

Согласно формуле 9 рассчитываем обобщенные скалярные оценки для каждой альтернативы. Результаты расчета для каждой из трех альтернатив:

- Q1 = – 8,825
- Q2 = – 15,066
- Q3 = – 10,183

Полученные в результате выполненных вычислений обобщенные скалярные оценки сравниваются между собой. Альтернатива Антивирус Dr.Web имеет наибольшую оценку и является наиболее рациональной среди данных альтернатив.

Значения обобщенных скалярных оценок могут принимать отрицательные значения, как в данном примере, в следствии того, что разные критерии имеют разные направления экстремума. Однако, опытным путем доказано, что количество оценок с разными направлениями экстремума не влияет на конечный результат нахождения наиболее рациональной альтернативы средства защиты информации.

В случае совпадений итоговый скалярных оценок нескольких альтернатив, рекомендуется внести дополнительный критерий, который помог бы сделать окончательный выбор в пользу той или иной альтернативы.

Процесс выбора наиболее рациональной альтернативы средства защиты из произвольного количества альтернатив по произвольному количеству критериев с помощью метода многокритериального выбора средств защиты информации, основанного на методике комплексной оценки структур, может быть реализован в виде программного кода, включающего в себя все перечисленные в статье этапы работы по методу.

Заключение

В статье предложен метод многокритериального выбора средств защиты информации, основанный на методике комплексной оценки структур, и представлен пример апробации данного метода с помощью выбора наиболее рациональной альтернативы из множества средств антивирусной защиты, представленных на рынке.

Метод позволяет осуществить рациональный выбор из произвольного количества альтернатив по произвольному количеству критериев. Отличительной особенностью метода является возможность учесть величину шага для частного критерия. Данный метод применим для количественных критериев, либо для критериев, которые были переведены из качественных в количественные.

Поскольку предложенный метод включает в себя большое количество этапов, а также сложные и трудоемкие расчеты, необходимо разработать программное средство, которое позволило бы автоматизировать все этапы метода многокритериального выбора средств защиты.

Дальнейшая работа будет направлена на автоматизацию метода и разработку программного средства, которое имело бы интуитивно понятный интерфейс для специалиста по информационной безопасности и позволило бы сократить время и трудозатраты на выбор рационального средства защиты из множества альтернатив с учетом их критериев.

Литература

1. Живицкая Е. Н. Системный анализ и проектирование [Электронный ресурс]. URL: http://victor-safronov.ru/systems-analysis/lectures/zhivickaya/21.html (дата обращения: 10.12.2024)

2. Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. 30 марта 1992, 29 с.

3. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных.

4. Государственный реестр сертифицированных средств защиты инфор-мации [Электронный ресурс]. URL: https://reestr.fstec.ru/reg3 (дата обращения: 10.12.2024).

5. Яндыбаева Э.Э., Машкина И.В. Разработка модели планирования используемых средств защиты информации для информационной системы электронной торговой площадки / // Вестник УГАТУ. – 2015. – Том 19, № 1 (67). – С. 264–269

References

1. Zhivitskaya E. N. Sistemnyy analiz i proektirovanie [Elektronnyy resurs]. URL: http://victor-safronov.ru/systems-analysis/lectures/zhivickaya/21.html (data obrashcheniya: 10.12.2024)

2. Rukovodyashchiy dokument Avtomatizirovannye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii. 30 marta 1992, 29 s.

3. Postanovlenie Pravitel'stva RF ot 01.11.2012 N 1119 "Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh.

4. Gosudarstvennyy reestr sertifitsirovannykh sredstv zashchity informatsii [Elektronnyy resurs]. URL: https://reestr.fstec.ru/reg3 (data obrashcheniya: 10.12.2024)

5. Yandybaeva E.E., Mashkina I.V. Razrabotka modeli planirovaniya ispol'zuemykh sredstv zashchity informatsii dlya informatsionnoy sistemy elektronnoy torgovoy ploshchadki / // Vestnik UGATU. – 2015. – Tom 19, № 1 (67). – S. 264–269

СЕНЦОВА Алина Юрьевна, кандидат технических наук, доцент кафедры вычислительной техники и защиты информации, федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий». 450076, Республика Башкортостан, г. Уфа, ул. Заки Валиди, д. 32. E-mail: sentsova.alina@yandex.ru

АРСЛАНОВА Гульназ Ильсуровна, студент кафедры вычислительной техники и защиты информации, федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий». 450076, Республика Башкортостан, г. Уфа, ул. Заки Валиди, д. 32. E-mail: arslanovagulnaz7@mail.ru

РУСИНОВА Дарья Сергеевна, студент кафедры вычислительной техники и защиты информации, федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский университет науки и технологий». 450076, Республика Башкортостан, г. Уфа, ул. Заки Валиди, д. 32. E-mail: rusinova_darya03@mail.ru

SENTSOVA Alina Yurievna, Candidate of Technical Sciences, Associate Professor of the Department of Computer Science and Information Security, Federal State Budgetary Educational Institution of Higher Education "Ufa University of Science and Technology". 450076, Republic of Bashkortostan, Ufa, Zaki Validi St., 32. E-mail: sentsova.alina@yandex.ru

ARSLANOVA Gulnaz Ilsurovna, student of the Department of Computer Science and Information Security, Federal State Budgetary Educational Institution of Higher Education "Ufa University of Science and Technology". 450076, Republic of Bashkortostan, Ufa, Zaki Validi St., 32. E-mail: arslanovagulnaz7@mail.ru

RUSINOVA Darya Sergeevna, student of the Department of Computer Engineering and Information Security, Federal State Budgetary Educational Institution of Higher Education "Ufa University of Science and Technology". 450076, Republic of Bashkortostan, Ufa, Zaki Validi St., 32. E-mail: rusinova_darya03@mail.ru