УДК 621.382, 519.226, 519.833

05.00.00 Технические науки

МЕТОДИКА ВЫБОРА СРЕДСТВ ЗАЩИТЫ ДЛЯ КОРПОРАТИВНОЙ СЕТИ

Петриченко Григорий Семенович
к. т. н., профессор
РИНЦ SPIN-код: 3093-4136
Кубанский государственный технологический университет, Краснодар, Россия, Petry_gr@mail.ru

Нарыжная Наталья Юрьевна
к. т. н.
РИНЦ SPIN-код: 2238-9501
Финансовый университет при правительстве Российской Федерации (Краснодарский филиал), Краснодар, Россия, NYUNaryzhnaya@fa.ru

Крицкая Лидия Михайловна
к. т. н., доцент
РИНЦ SPIN-код: 6078-7509
Кубанский государственный технологический университет, Краснодар, Россия, Petri61@mail.ru

В настоящее время в связи с высокими требованиями к устойчивости функционирования сетей и их информационной безопасностью актуальной проблемой является выбор на рынке программно-аппаратных продуктов, средств защиты информации от различного ряда угроз, возникающих в корпоративной сети предприятия. Несмотря на то, что рынок программно-аппаратных продуктов предлагает много средств защиты информации, руководителям и экспертам пока сложно разобраться, чем они отличаются друг от друга, и какими принципами следует руководствоваться при их выборе. В статье для решения задачи выбора средств защиты, их покупки и установки на рабочие станции и сервера корпоративной сети, предлагается применить комплексную методику, основанную на методах теории игр и анализа иерархий

Ключевые слова: ПРИНЯТИЕ РЕШЕНИЯ, РИСК, ТЕОРИЯ ИГР, ИГРЫ С ПРИРОДОЙ, МЕТОД АНАЛИЗА ИЕРАРХИЙ, ПРИОРИТЕТНОСТЬ, ЗАЩИТА ИНФОРМАЦИИ, КОРПОРАТИВНАЯ СЕТЬ

Doi: 10.21515/1990-4665-121-130

UDC 621.382, 519.226, 519.833

Technical sciences

THE TECHNIQUE OF A SECURITY TOOLS CHOICE FOR A CORPORATE NETWORK

Petrychenko Grigoriy Semenovich
Cand.Tech.Sci., professor
RSCI SPIN code: 3093-4136
Kuban State University of Technology, Krasnodar, Russia, Petry_gr@mail.ru

Naryzhnaya Nataliya Yurievna
Cand.Tech.Sci.
RSCI SPIN code: 2238-9501
Financial University under the Government of the Russian Federation (Krasnodar branch), Krasnodar, Russia, NYUNaryzhnaya@fa.ru

Kritskaya Lidiya Michailovna
Cand.Tech.Sci., associate professor
RSCI SPIN code: 6078-7509
Kuban State University of Technology, Krasnodar, Russia, Petri61@mail.ru

At the present time, due to the high demands on the stability of the networks and information security, the actual problem is the choice in the market of software and hardware products, the protection of information assets from a number of different threats that arise in the corporate network. Despite the fact that the market for hardware and software products offers a lot of information security, it is difficult to leaders and experts to find out how they differ from each other, and what principles should guide their choice. In the article, for solving the problem of the choice of remedies, their purchase and installation on workstations and enterprise network servers, it is proposed to use a comprehensive methodology, based on the methods of the game theory and the analysis of hierarchies

Keywords: DECISION-MAKING, RISK, GAME THEORY, GAMES WITH NATURE, THE METHOD OF ANALYSIS OF HIERARCHIES, PRIORITY, DATA PROTECTION, CORPORATE NETWORK

Существующие угрозы корпоративных сетей

Актуальными специфическими угрозами для корпоративных сетей являются:

1. Несанкционированный доступ к данным серверов, рабочих станций и виртуальных машин путем их уязвимости.
2. Заражение и модификация программного обеспечения и информации серверов, рабочих станций и виртуальных машин вредоносным программным обеспечением.
3. Потери производительности корпоративной сети и отказ серверов в обслуживании запросов рабочих станций и т.д.

Постановка задачи

Для проведения сравнительной оценки различных средств защиты информации, можно использовать обобщенный показатель, включающий в себя частные показатели средств защиты информации.

В общем случае обобщенный показатель средств защиты информации, может быть представлен в виде следующего выражения:

$$W_i = \sum_{j=1}^{n} a_{ij} q_j, \quad (1)$$

где a_{ij} − относительные значения частных показателей средств защиты (критериев); q_j − веса критериев.

Наилучшее средство защиты информации будет, определятся, из выражения:

$$W_i^{*} = \max W_i \ . \quad (2)$$

Для проверки правильности нашего выбора, необходимо составить матрицу рисков используя основные положения теории игр и критерия Байеса:

$$R_i = \sum_{j=1}^{n} r_{ij} q_j \ , \quad (3)$$

где $\{r_{ij}\}$ − матрица рисков.

Оптимальное средство защиты информации будет определяться по минимальному показателю неэффективности:

$$R_i^o = \min R_i . \quad (4)$$

Решение задачи

Комплексная методика включает следующие этапы: определение частных показателей (критериев) средств защиты и вычисление их относительных значений [1]; вычисление весовых коэффициентов критериев на основе применения метода анализа иерархий [2, 3]; выбор средств защиты на основе применения основных положений теории игр.

Рассмотрим комплексную методику выбора средств защиты информации на наглядном примере. Пусть перед фирмой стоит задача по выбору средств защиты для корпоративной сети из пяти имеющихся $СЗИ_1$, $СЗИ_2$, …, $СЗИ_5$ на рынке программных и аппаратных продуктов.

Выбор средств защиты информации можно осуществить по самым разным критериям:

1. K_1 – функциональные требования. Данный критерий определяет механизм безопасности, реализуемый средством защиты информации, требование гарантий, документирование всех событий, происходящих в системе.
2. K_2 – наличие межсетевого экрана.
3. K_3 – способность управлять потоками информации между компонентами виртуальной инфраструктуры и осуществлять управление доступом субъектов доступа к объектам в виртуальной инфраструктуре.
4. K_4 – мониторинг и фильтрация почтового трафика (контекстный анализ).
5. K_5 – стоимость.

Этап 1. Определение частных показателей (критериев) средств защиты и вычисление их относительных значений.

На первом этапе вычисления определяют относительное значение одного и того же частного показателя для различных средств защиты

информации. Каждое значение частного показателя средств защиты информации делят на наилучшее и получают относительное значение частного показателя. Аналогично вычисляют относительные оценки для всех частных показателей средств защиты информации (СЗИ) и составляют таблицу.

В таблице 1 представлены баллы, выставленные экспертами средствам защиты информации по каждому частному показателю (критерию).

Таблица 1 – Экспертные баллы

	Частные показатели (критерии) средств защиты информации				
$СЗИ_i$	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$
$СЗИ_1$	5	7	8	4	3
$СЗИ_2$	3	2	5	8	9
$СЗИ_3$	4	7	6	3	2
$СЗИ_4$	7	1	8	9	4
$СЗИ_5$	5	3	9	4	2

В таблице 2 представлены относительные оценки для всех частных показателей средств защиты информации.

Таблица 2 – Относительные оценки

	Частные показатели (критерии) средств защиты информации				
$СЗИ_i$	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$
$СЗИ_1$	0,625	0,875	1	0,5	0,375
$СЗИ_2$	0,333333333	0,222222222	0,555555556	0,888888889	1
$СЗИ_3$	0,571428571	1	0,857142857	0,428571429	0,285714
$СЗИ_4$	0,777777778	0,111111111	0,888888889	1	0,444444
$СЗИ_5$	0,555555556	0,333333333	1	0,444444444	0,222222

Этап 2. Вычисление весовых коэффициентов критериев на основе применения метода анализа иерархий.

Необходимо осуществить заполнение квадратной матрицы парных сравнений критериев по следующему правилу (табл. 3).

Матрицы критериев попарных сравнений обладают свойством обратной симметрии, т.е.:

$$k_{ij}^{*} = 1/k_{ji}^{*}\ , \qquad (5)$$

где $k_{ij}^{*} = \lambda_i / \lambda_j$; λ_i, λ_j − экспертные оценки элементов $K_1, K_2, ..., K_n$; i,j – индексы относятся к строке и столбцу.

Таблица 3 − Матрица парных сравнений

	K_1	K_2	...	K_n
K_1	λ_1 / λ_1	λ_1 / λ_2	...	λ_1 / λ_n
K_2	λ_2 / λ_1	λ_2 / λ_2	...	λ_2 / λ_n
...	...	...	...	...
K_n	λ_n / λ_1	λ_n / λ_2	...	λ_n / λ_n

Результаты парных сравнений (5) отражают превосходство одного критерия над другим, при этом рекомендуется использовать шкалу относительной важности (табл.4).

Таблица 4 – Шкала относительной важности

Интенсивность относительной важности	Определение
1	Равная важность
3	Умеренное превосходство одного над другим
5	Существенное или сильное превосходство
7	Значительное превосходство
9	Очень сильное превосходство
2, 4, 6, 8	Промежуточные решения между двумя соседними суждениями
Обратные величины приведенных выше чисел	Если при сравнении одного элемента с другим получено одно из вышеуказанных чисел (например, 7), то при сравнении второго элемента с первым получим обратную величину (т.е. 1/7)

В результате экспертного оценивания по правилу (5) была построена таблица 5, вычислены оценки компонентов собственного вектора, а также получены нормализованные результаты оценки вектора приоритетов.

Для получения оценки вектора приоритетов, необходимо сначала вычислить компоненты собственного вектора по строкам матрицы.

Процедура определения собственных векторов состоит из перемножения n-элементов в строке матрицы и извлечения корня n-й степени из перемноженных элементов (т.е. геометрической средней по строкам матрицы). Полученный таким образом столбец чисел нормализуется делением каждого числа на сумму элементов собственного вектора. Нормализованный столбец чисел и будет являться вектором приоритетов (см. табл. 5).

Таблица 5 – Оценки компонентов собственного вектора

Критерии	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$	Оценки компонентов собственного вектора	Нормализованные оценки вектора приоритетов - q_i
$К_1$	1	3	0,333333	5	7	2,036168	0,263834
$К_2$	0,333333	1	0,2	3	5	1	0,129574
$К_3$	3	5	1	7	9	3,936283	0,510039
$К_4$	0,2	0,333333	0,142857	1	3	0,491119	0,063636
$К_5$	0,142857	0,2	0,111111	0,333333	1	0,254047	0,032918
Сумма						7,717617	1
Lmax= 5,242932129			ИС=0,060733032			ОС=0,104712125	

Мера согласованности относительных оценок может быть выражена с помощью индекса согласованности. Согласованность локальных приоритетов проверим путем вычисления индекса согласованности (ИС) и отношения согласованности (ОС). Для индекса согласованности имеем

$$ИС = (\lambda_{max} - n)/(n-1), \quad (6)$$

где n – число сравниваемых элементов матрицы;

λ_{max} – максимальное собственное значение рассматриваемой матрицы суждений.

Отношение согласованности получаем путем деления значения ИС на число, соответствующее случайной согласованности матрицы того же порядка (см. табл. 6).

Величина ОС должна быть порядка 10% или менее, чтобы быть приемлемой. В некоторых случаях допускается 20%, но не более. Если ОС выходит за эти пределы, то необходимо вновь исследовать задачу и проверить все суждения.

Таблица 6 – Соответствие порядка матрицы и среднего значения случайного индекса

Размер матрицы	1	2	3	4	5	6	7	8	9	10
Случайная согласованность	0	0	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49

Приоритет среди весовых коэффициентов критериев имеют $К_3$=0,510039 и $К_1$=0,263834.

Этап 3. Выбор средств защиты на основе применения основных положений теории игр.

Выбор средств защиты информации можно выполнить на основе обобщенного показателя (1). Результаты выбора представлены в таблице 7.

Таблица 7 – Обобщенный показатель средств защиты информации

	Относительные значения частных показателей (критериев) - a_{ij}					
СЗИ	$К_1$	$К_2$	$К_3$	$К_4$	$К_5$	W_i
$СЗИ_1$	0,625	0,875	1	0,5	0,375	0,832475
$СЗИ_2$	0,333333	0,222222	0,555556	0,888889	1	0,489577
$СЗИ_3$	0,571429	1	0,857143	0,428571	0,285714	0,75419
$СЗИ_4$	0,777778	0,111111	0,888889	1	0,444444	0,751236
$СЗИ_5$	0,555556	0,333333	1	0,444444	0,222222	0,735403
q_j	0,263834	0,129574	0,510039	0,063636	0,032918	

В результате выбора первое место среди средств защиты занимает $СЗИ_1$ с максимальным обобщенным показателем 0,832475, которое будет предлагаться для покупки и установки на рабочие станции и сервера корпоративной сети предприятия.

Для проверки правильности нашего выбора, составим матрицу рисков.

Матрицу рисков составим на основе таблицы относительных оценок для всех частных показателей средств защиты информации (табл. 2).

Средства защиты информации СЗИ$_i$ назовем стратегиями, а частные показатели (критерии) – показателями природы. Применим основные положения теории игр [4] для составления таблицы рисков и сформулируем определение игры с природой.

Показателем благоприятности состояния K_j природы для увеличения выигрыша называется наибольший выигрыш фирмы при этом состоянии природы, то есть наибольший элемент в j-ом столбце таблицы 8:

$$\beta_j = \max(a_{ij}) \quad , \text{j=1,2,…,n.} \tag{7}$$

Для характеристики «удачности» применения фирмой стратегии СЗИ$_i$ в состоянии природы K_j введем понятие риска.

Риском r_{ij} фирмы при выборе стратегии СЗИ$_i$, будем называть разность между показателями благоприятности β_j в состоянии природы K_j и выигрышем a_{ij}:

$$r_{ij} = \beta_j - a_{ij}. \tag{8}$$

Риском в нашем случае будет называться упущенная возможность получения максимального выигрыша в данном состоянии природы K_j, где $r_{ij} \geq 0$. Верхняя граница рисков для каждого состояния природы K_j определяется из следующего выражения:

$$W_j = \min(a_{ij}), \text{ j=1,2,…,n,} \tag{9}$$

где W_j − минимальный выигрыш при данном состоянии природы.

Колебание выигрыша в заданном состоянии природы K_j, будет определятmся следующим выражением:

$$\Delta r_{ij} = \beta_j - W_j, \quad (10)$$

если $a_{ij} = W_j$, то риск в нашем случае будет максимальным. Таким образом, по критерию риска эта стратегия выбранная фирмой, будет наихудшей.

Преобразуем таблицу 2, применяя выражение (7) в платежную матрицу и получим матрицу игры, которая представлена в таблице 8.

Таблица 8 – Матрица игры

		Состояния природы K_j				
СТРАТЕГИИ	СЗИ$_i$	К$_1$	К$_2$	К$_3$	К$_4$	К$_5$
	СЗИ$_1$	0,625	0,875	1	0,5	0,375
	СЗИ$_2$	0,333333	0,222222	0,555556	0,888889	1
	СЗИ$_3$	0,571429	1	0,857143	0,428571	0,285714
	СЗИ$_4$	0,777778	0,111111	0,888889	1	0,444444
	СЗИ$_5$	0,555556	0,333333	1	0,444444	0,222222
	β_j	0,777778	1	1	1	1

На основании таблицы 8 и выражения (10) построим матрицу рисков.

Таблица 9 – Матрица рисков

		Состояния природы K_j					
СТРАТЕГИИ	СЗИ$_i$	*К$_1$*	*К$_2$*	*К$_3$*	*К$_4$*	*К$_5$*	R_i
	СЗИ$_1$	0,152778	0,125	0	0,5	0,625	0,108896
	СЗИ$_2$	0,444444	0,777778	0,444444	0,111111	0	0,451794
	СЗИ$_3$	0,206349	0	0,142857	0,571429	0,714286	0,187181
	СЗИ$_4$	0	0,888889	0,111111	0	0,555556	0,190136
	СЗИ$_5$	0,222222	0,666667	0	0,555556	0,777778	0,205969
	q_j	0,263834	0,129574	0,510039	0,063636	0,032918	

Таким образом, на основании матрицы рисков согласно выражению (4) первое место занимает стратегия номер 1 с минимальным показателем неэффективности R_1= 0,108896. Фирме рекомендуется остановить свой

выбор на покупке и установке на рабочие станции корпоративной сети предприятия $СЗИ_1$.

Список литературы

1. Петриченко, Г.С. Оценка эффективности программного обеспечения / Г.С. Петриченко, В.Г. Петриченко // Научные ведомости Белгородского государственного университета. Серия: Экономика, Информатика. − 2016. − № 9 (230). − вып. 38. С. 108-112.

2. Петриченко, Г.С. Построение программы поиска неисправностей в электронных блоках средств вычислительной техники с применением метода анализа иерархий / Г.С. Петриченко, Н.Ю. Нарыжная, М.Ю. Срур // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. − 2011. − № 69. − С. 13-22.

3. Саати, Т. Принятие решений. Метод анализа иерархий / Т. Саати. − М.: Радио и связь, 1993.

4. A Beautiful Mind: A Biography of John Forbes Nash, Jr., Winner of the Nobel Prize in Economics Simon & Schuster, 1994. ISBN 0-684-81906-6.

References

1. Petrichenko, G.S. Ocenka jeffektivnosti programmnogo obespechenija / G.S. Petrichenko, V.G. Petrichenko // Nauchnye vedomosti Belgorodskogo gosudarstvennogo universiteta. Serija: Jekonomika, Informatika. - 2016. - № 9 (230). - vyp. 38. S. 108-112.

2. Petrichenko, G.S. Postroenie programmy poiska neispravnostej v jelektronnyh blokah sredstv vychislitel'noj tehniki s primeneniem metoda analiza ierarhij / G.S. Petrichenko, N.Ju. Naryzhnaja, M.Ju. Srur // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta. ¬- 2011. - № 69. - S. 13-22.

3. Saati, T. Prinjatie reshenij. Metod analiza ierarhij / T. Saati. – M.: Radio i svjaz', 1993.

4. A Beautiful Mind: A Biography of John Forbes Nash, Jr., Winner of the Nobel Prize in Economics Simon & Schuster, 1994. ISBN 0-684-81906-6.