Оценка эффективности системы экономической безопасности

УДК 351.863

Кавун С. В.

Рассматривается задача оценки эффективности системы экономической безопасности (СЭБ), интерпретируемая как оптимизационная задача. Для получения оценок промежуточных показателей предлагаются реальные показатели функционирования СЭБ при реализации комплексной стратегии развития предприятия на основе концепции экономической безопасности.

В эпоху мирового финансового и экономического кризиса рыночные отношения, складывающиеся в процессе функционирования предприятия, приобретают совершенно другой смысл. Его глобальная идея состоит в том, что используемые ранее известные подходы и концепции сегодня не оправдывают своей сути. Тому примером могут служить различные статистические и аналитические исследования известных мировых компаний, как например, CSI (их известный отчет Computer Crime and Security Survey), Perimetrix, RSA, Finjan, IT Policy Compliance Group, «Эрнст энд Янг», Ponemon Institute и др. Все представляемые ими результаты свидетельствуют о динамическом повышении уровня потерь (финансовых, экономических, производственных, трудовых и др.). Это весьма негативно сказывается на общем экономическом развитии предприятий. Следствием данных событий часто являются банкротства самих предприятий, резкое снижение эффективности производства, глобальные сокращения рабочих мест, поглощения мелких предприятий крупными и др. негативные экономические процессы.

Предприятия, пытаясь "выжить" в сложившихся условиях рассматривают различные механизмы выхода из кризиса. Одним из таких механизмов, несомненно, является разработка и принятие (внедрение) новой концепции экономической безопасности (КЭБ), которая учитывает всю динамику происходящих процессов. Однако, большинство существующих подходов [1, 2] являются либо статическими, либо основываются на показателях, реально получить которые не представляется возможным.

Таким образом, в разрабатываемой КЭБ, осуществляется попытка ввести глобальный фактор динамики с учетом реальных количественных показателей.

В основе КЭБ на предприятии лежит система ЭБ (СЭБ), реализация которой в большей степени и определяет стратегию дальнейшего функционирования и развития предприятия. Идеология разработки СЭБ на предприятии описана в работе [3].

Поскольку для руководителя любого звена управления (CISO, CSO, CFO, CEO и др.) особенно актуальным является вопрос эффективности реализации и внедрения управленческого решения, то возникает необходимость оценки эффективности СЭБ.

Для получения этой оценки введем понятие уровня эффективности СЭБ и обозначим его как **LEES (level of efficiency of economic security)**. А поскольку КЭБ реализует динамическую модель, то, основываясь на жизненном цикле СЭБ, получим выражение

$$\mathbf{LEES} = \max\{\mathbf{LEES_h}\} \qquad (1)$$

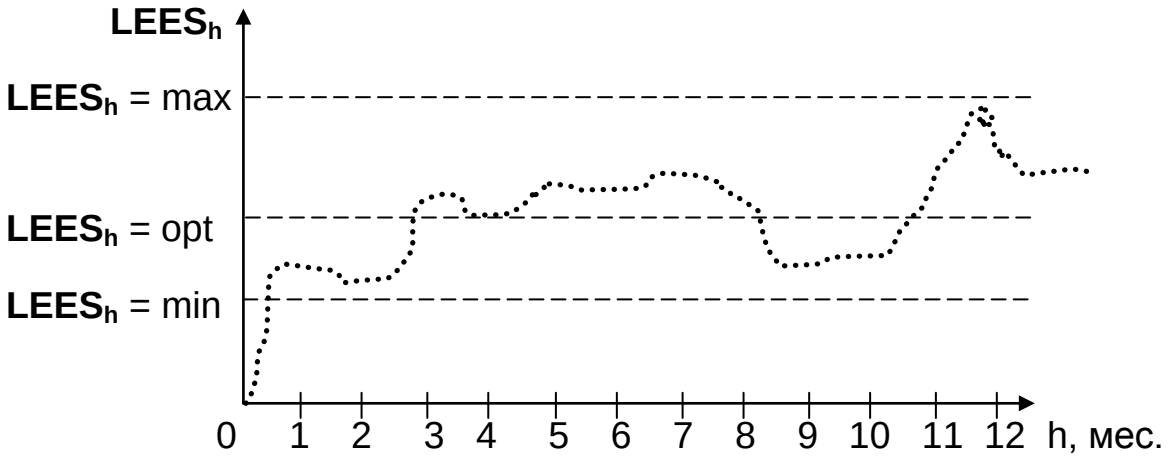

Рис. 1. **Динамика учета уровня эффективности СЭБ**

где $\mathbf{LEES_h}$ – значение уровня эффективности СЭБ в момент времени h, если принять длительность исследования в один год и периодичность расчета 1 раз в месяц, то графически зависимость будет выглядеть, как показано на рис. 1.

Кроме того, очевидна функциональная зависимость уровня эффективности СЭБ от различных факторов развития предприятия [4]. Тогда при ее учете получим зависимость

$$\mathbf{LEES_h = f\ (T_{ср},\ \overline{T_z^B}\ [4],\ V_{ст},\ V_{УКУ},\ V_{ВСШФ},\ V_{НД},\ V_{АР},\ V_{АИ})},\qquad (2)$$

или

$$\mathbf{LEES_h = f\ (T_{ср},\ \overline{T_z^B},\ V_{ST},\ V_{VCO},\ V_{VSSF},\ V_{ND},\ V_{AR},\ V_{AII})}\qquad (3)$$

или

$$\mathbf{LEES_h = f\ (\overline{T},\ \overline{T_z^B},\ V_{SES})}.\qquad (4)$$

Причем $\overline{T} \rightarrow$ max, $\overline{T_z^B}$, $\rightarrow$ min, $V_{SES} \rightarrow$ min.

Где

$$T_{ср} = \overline{T} = \frac{1}{\frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{K} IES_{ij}},$$

$T_{ср}$ – среднее время между инцидентами в области ЭБ;

N – количество отчетных периодов, как правило, N = 12 – по количеству месяцев и длительности исследования в один год;

К – количество видов (типов) экономических преступлений [2];

IES_{ij} – частота инцидентов в области ЭБ (incident of economic security) за i-й период j-го вида (типа) экономического преступления [2];

$\overline{T_z^B}$ – среднее время восстановления z-го узла СЭБ

$$\overline{T_z^B} = \frac{1}{N}\sum_{j=1}^{N} t_{zj}^B,$$

t_{zj}^B - время восстановления z-го узла СЭБ за j-й период;

$V_{ст}$ (V_{ST} – standards) – объем подсистем (бизнес-процессов), выполняющих требования каких-либо стандартов ЭБ, определяют соответствующие затраты на реализацию стандартов ЭБ, общее количество должно быть не менее 30%;

$V_{УКУ}$ (V_{VCO} – vulnerabilities, channel of outflow) – объем подсистем (бизнес-процессов), на которых выполнен анализ уязвимостей и каналов утечки информации с ограниченным доступом, определяют соответствующие затраты на проведение анализа, общее количество должно быть не менее 28%;

$V_{ВСШФ}$ (V_{VSSF} – antivirus, antispam, antispyware, firewalls) – объем подсистем (бизнес-процессов), для которых установлены антивирусные, антиспамовые, антишпионские средства и программы-файерволы,

определяют соответствующие затраты на приобретение, установку и сопровождение, общее количество должно быть не менее 12%;

$V_{НД}$ (V_{ND} – normative documents) – объем подсистем (бизнес-процессов), для которых разработаны и внедрены нормативные документы (инструкции, приказы, правила), определяют соответствующие затраты на разработку и внедрение системы документооборота, общее количество должно быть не менее 15%;

V_{AP} (V_{AR} – audit and level of risks) – объем подсистем (бизнес-процессов), для которых выполнен аудит, проведен и оценен уровень рисков, определяют соответствующие затраты на реализацию указанных мероприятий, общее количество должно быть не менее 10%;

V_{All} – объем оставшихся подсистем (бизнес-процессов), определяют соответствующие затраты на их реализацию, общее количество должно быть не менее 5%;

$V_{СЭБ}$ (V_{SES} – system of economic security (safety)) – объем (сумма) всех подсистем (бизнес-процессов), определяют соответствующие единовременные затраты.

Тогда

$$\mathbf{V_{СЭБ} = V_{ст} + V_{УКУ} + V_{ВСШФ} + V_{НД} + V_{AP} + V_{All} = 100\%,}$$

$$\mathbf{V_{SES} = V_{ST} + V_{VCO} + V_{VSSF} + V_{ND} + V_{AR} + V_{All} = 100\%.}$$

В графическом виде с учетом доли определенных компонент, полученной в результате экспертного опроса распределение $\mathbf{V_{SES}}$ будет иметь вид, представленный на рис. 2.

Реально, подобное распределение не оказывает существенного влияния на определение уровня эффективности СЭБ, что будет видно в дальнейшем. Кроме того, для указанных типов затрат должно выполняться следующее условие, обеспечивающее целесообразность и необходимость реализации СЭБ на предприятии.

Если $V_{All} > V_{ST} + V_{VCO} + V_{VSSF} + V_{ND} + V_{AR}$, то оценивать эффективность СЭБ не целесообразно, т.к. затраты на реализацию и поддержание оставшихся подсистем СЭБ превысят затраты, имеющие положительное сальдо для СЭБ.

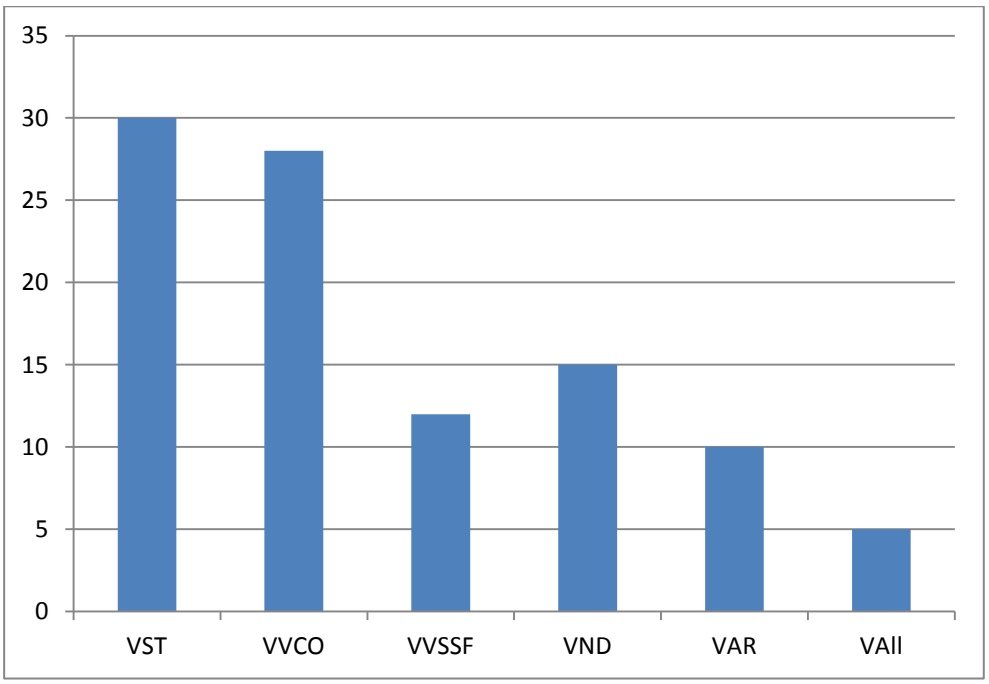

Рис. 2. **Распределение объема единовременных затрат**

При использовании оптимизационного подхода к получаемой оценке эффективности СЭБ выражение (3) будет преобразовано в:

$$LEES = \begin{cases} \overline{T} \to max \\ \overline{T_z^B} \to min \\ \mathrm{V_{ST}} \to max \\ \mathrm{V_{VCO}} \to max \\ \mathrm{V_{VSSF}} \to max \\ \mathrm{V_{ND}} \to max \\ \mathrm{V_{AR}} \to max \\ \mathrm{V_{All}} \to min \end{cases}. \quad (5)$$

Для обеспечения возможности реального расчета уровня эффективности СЭБ необходимо ввести технические показатели СЭБ, которые бы обеспечили возможность динамического их получения автоматизированным способом. Их перечень представлен ниже.

K_{PC} – количество рабочих станций (workstations, personal computers), участвующих в обеспечении функционирования СЭБ, если предположить, что в среднем 85% [1] сотрудников (M) на современном предприятии имеют на рабочем месте компьютеры, а также с учетом того, что $V_{ST} = \{V_{VCO}\} \cup \{V_{VSSF}\} \cup \{V_{AR}\}$, то

$$\mathbf{K_{PC} = \lceil 0{,}85 \times M \rceil}.$$

K_S – количество серверов (servers), участвующих в обеспечении функционирования СЭБ, если предположить, что в среднем на 20-25 рабочих станций приходится один сервер, то

$$\mathbf{K_S = \lfloor K_{PC} / 25 \rfloor.}$$

K_{NE} – количество единиц сетевого оборудования (network equipment), участвующих в обеспечении функционирования рабочих станций и серверов, при условии, что количество портов для подключения сетевого оборудования Z = 5,8,12,16,32,64, в зависимости от фирмы производителя и технических характеристик сетевого оборудования, то

$$\mathbf{K_{NE} = \lceil (K_{PC} + K_S)/Z \rceil.}$$

K_{CE} – количество коммуникационного оборудования (communication equipment), участвующих в обеспечении деятельности сотрудников предприятия (КПК, сотовые телефоны, коммуникаторы, смартфоны, netbook, miniPC), поэтому, в простейшем случае, K_{NE} равно количеству сотрудников (M), однако, с учетом того, что каждый 5-й сотрудник имеет несколько подобных устройств [2], то

$$\mathbf{K_{CE} = 0{,}2 \times M + M = \lceil 1{,}2 \times M \rceil.}$$

K_{CTI} – количество трактов передачи информации (channel of transfer information), образующих каналы утечки информации (КУИ), классификация которых представлена в табл. 1.

Тогда при использовании введенного классификатора количество КУИ будет определяться по формуле:

$$\mathbf{K_{CTI} = \lceil (16 + K_{NE}) \times (K_{PC} + K_S) + 9 \times K_{CE} + 2 \times K_F + K_T \rceil,} \qquad (6)$$

где K_T – количество стационарных телефонов (telephones),

K_F – количество стационарных факсов (faxes), причем факс имеет два КУИ: акустический и передачи данных.

Тогда с учетом введенных показателей система (5) примет вид:

$$LEES = \begin{cases} \overline{T} \to max \\ \overline{T_z^B} \to min \\ \mathrm{K_{PC}} \to opt(min) \\ \mathrm{K_S} \to min \\ \mathrm{K_{NE}} \to min \\ \mathrm{K_{CE}} \to min \\ \mathrm{K_{CTI}} \to min \end{cases}. \qquad (7)$$

Таблица 1

Классификация КУИ

Тип устройства	№ п/п	Тип КУИ
ПК и сервер	1.	электронная почта
	2.	FTP-сервис
	3.	HTTP-сервис
	4.	P2P-сервис
	5.	CHAT-сервис
	6.	ICQ-сервис
	7.	IRC-сервис
	8.	Wi-Fi-канал
	9.	IrDA-канал
	10.	Bluetooth-канал
	11.	WWW-сервис
	12.	USB- интерфейс
	13.	COM- интерфейс
	14.	LPT- интерфейс
	15.	FDD-интерфейс
	16.	HDD-интерфейс
	17.	simple copying (простое копирование по сети, используя множество $\{K_{NE}\}$)
сотовые телефоны и им подобные устройства	1.	Wi-Fi-канал
	2.	IrDA-канал
	3.	ICQ-сервис
	4.	CHAT-сервис
	5.	IRC-сервис
	6.	USB-канал
	7.	HTTP-сервис
	8.	Bluetooth-канал
	9.	электронная почта

Основываясь на возможности поглощения на основании выражения (6) и направленности оптимизации (min) можно получить минимизацию системы (7), тогда

$$LEES = \begin{cases} \overline{T} \to max \\ \overline{T_z^B} \to min \\ \mathrm{K_{CTI}} \to min \end{cases}, \quad (8)$$

или в линейном виде

$$LEES = \max(\overline{T}) \min\left(\overline{T_z^B}, \mathrm{K_{CTI}}\right). \quad (9)$$

Если привести выражения (8-9) к единому оптимуму, то получим

$$LEES = \begin{cases} (1-\overline{T}) \to min \\ \overline{T_z^B} \to min \\ \mathrm{K_{CTI}} \to min \end{cases}, \quad (10)$$

$$LEES = \min\left((1-\overline{T}), \overline{T_z^B}, \mathrm{K_{CTI}}\right). \quad (11)$$

Таким образом, задача оценки эффективности СЭБ сформулирована как многокритериальная (трехфакторная) задача оптимизации.

Если ввести дополнительно фактор времени, т.е. учесть динамику оценки эффективности СЭБ, то также необходимо ввести нормирование всех промежуточных факторов. Тогда справедливы соотношения:

$$\begin{cases} \sum_{i=1}^{N} T_{CP}^i = 365, \\ \sum_{i=1}^{N} {}^{H}T_{CP}^i = 1, \end{cases} \quad \begin{cases} \sum_{i=1}^{365/N} IES_{ij} < 365, \\ \sum_{i=1}^{365/N} {}^{H}IES_{ij} = 1, \end{cases} \quad \begin{cases} \overline{{}_{i}T_z^B} \times \frac{1}{N} \sum_{i=1}^{N} IES_{ij} < 365, \\ \sum_{i=1}^{N} \overline{{}_{i}^{H}T_z^B} = 1, \end{cases}$$

$$\begin{cases} V_{SES} = \frac{1}{N} \sum_{i=1}^{N} V_{SES}^i \\ \sum_{i=1}^{N} V_{ST}^i + \sum_{i=1}^{N} V_{VCO}^i + \sum_{i=1}^{N} V_{VSSF}^i + \sum_{i=1}^{N} V_{ND}^i + \sum_{i=1}^{N} V_{AR}^i + \sum_{i=1}^{N} V_{All}^i = N \times V_{SES} \\ \sum_{i} V_{SES}^i = \sum_{i} V_{SES}^{i+1} \\ \sum_{i=1}^{N} {}^{H}V_{ND}^i = 1, \sum_{i=1}^{N} {}^{H}V_{AR}^i = 1, \sum_{i=1}^{N} {}^{H}V_{All}^i = 1, \\ \left(V_{ST}^i + V_{VCO}^i + V_{VSSF}^i + V_{ND}^i + V_{AR}^i + V_{All}^i\right) = V_{SES} \text{ для } \forall\, i \\ V_{All}^i = V_{SES}^{i+1} - \sum_{i=1}^{N} \left(V_{ST}^i + V_{VCO}^i + V_{VSSF}^i + V_{ND}^i + V_{AR}^i\right) \\ \sum_{i=1}^{N} {}^{H}V_{ST}^i = 1, \sum_{i=1}^{N} {}^{H}V_{VCO}^i = 1, \sum_{i=1}^{N} {}^{H}V_{VSSF}^i = 1, \end{cases}$$

$$\begin{cases} K_{PC} + K_S < M, \\ K_{PC} + K_S \ll V_{SES} \\ \{V_{All}\} \neq K_S \end{cases}$$

Кроме того, для реализации СЭБ на предприятии необходимо соблюдение следующих условий:

1. Если $\overline{T_z^B} \geq T_{ср}$, то СЭБ считается утратившей свою работоспособность и не подлежит восстановлению, т.е. за время восстановления i-го узла возникает очередной инцидент.

2. Если $IES_{ij} \geq i$, то СЭБ считается утратившей свою работоспособность и не подлежит восстановлению, т.е. период времени, в течении которого возникает определенное количество инцидентов соответствует длительности текущего периода функционирования СЭБ, вследствие чего предприятие не функционирует.

3. Если $\overline{T_z^B} \geq \frac{1}{IES_{ij}}$, то СЭБ считается утратившей свою работоспособность и не подлежит восстановлению, т.к. среднее время восстановления системы после одного инцидента превышает время до наступления следующего инцидента.

В результате проведения реального исследования по оценке уровня эффективности СЭБ на предприятии будут получены данные, представленные для примера в табл. 2.

Таблица 2

Пример полученных данных исследования

период / параметр	i=1..12												
	январь	февраль	март	апрель	май	июнь	июль	август	сентябрь	октябрь	ноябрь	декабрь	сумма
1	2	3	4	5	6	7	8	9	10	11	12	13	14
T_{CP}^{i}, суток	48	25	28	19	40	23	24	23	45	29	23	38	365
${}^{H}T_{CP}^{i}$	0,13	0,07	0,08	0,05	0,11	0,06	0,07	0,06	0,13	0,08	0,06	0,10	1
IES_{ij} за месяц	0	1	0	2	1	3	6	13	0	2	3	4	35

Окончание табл. 2

1		2	3	4	5	6	7	8	9	10	11	12	13	14
$^{H}IES_{ij}$		0,00	0,03	0,00	0,06	0,03	0,09	0,16	0,37	0,00	0,06	0,09	0,11	1
$\overline{{}_{i}T_{z}^{B}}$, часов		0	1	0	3	2	5	9	27	0	2	8	7	64
$\overline{{}_{i}^{H}T_{z}^{B}}$		0,00	0,02	0,00	0,05	0,03	0,08	0,14	0,41	0,00	0,03	0,13	0,11	1
V_{SES} = 66	V_{ST}	5	5	5	6	6	6	6	7	7	7	8	8	76
	$^{H}V_{ST}$	0,07	0,07	0,07	0,08	0,08	0,08	0,08	0,08	0,08	0,09	0,11	0,11	1
	V_{VCO}	2	3	5	6	7	7	7	8	8	8	10	12	83
	$^{H}V_{VCO}$	0,02	0,04	0,06	0,07	0,09	0,08	0,08	0,10	0,10	0,10	0,12	0,14	1
	V_{VSSF}	10	13	13	17	18	18	18	18	18	18	19	23	203
	$^{H}V_{VSSF}$	0,05	0,06	0,07	0,08	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,11	1
	V_{ND}	1	1	1	2	2	3	6	7	8	11	11	11	64
	$^{H}V_{ND}$	0,02	0,02	0,02	0,03	0,03	0,05	0,09	0,11	0,13	0,17	0,16	0,17	1
	V_{AR}	6	6	6	6	6	6	6	6	7	7	7	7	76
	$^{H}V_{AR}$	0,08	0,08	0,08	0,08	0,08	0,08	0,08	0,08	0,09	0,09	0,09	0,09	1
	V_{All}	42	38	36	29	27	26	23	20	18	15	11	5	290
	$^{H}V_{All}$	0,14	0,13	0,12	0,10	0,09	0,09	0,08	0,07	0,06	0,05	0,04	0,02	1
K_{PC}		23	23	23	23	23	23	23	23	23	23	23	23	276
$^{H}K_{PC}$		0,09	0,08	0,08	0,08	0,08	0,09	0,09	0,08	0,08	0,08	0,08	0,09	1
K_{S}		1	1	1	1	1	1	1	1	1	1	1	1	12
$^{H}K_{S}$		0,08	0,08	0,08	0,09	0,08	0,09	0,08	0,09	0,08	0,08	0,09	0,08	1
K_{NE} (Z=16)		2	2	2	2	2	2	2	2	2	2	2	2	24
$^{H}K_{NE}$		0,09	0,08	0,08	0,08	0,08	0,09	0,09	0,08	0,08	0,08	0,08	0,09	1
K_{CE} (M=27)		32	32	32	32	32	32	32	32	32	32	32	32	384
$^{H}K_{CE}$		0,09	0,08	0,08	0,08	0,08	0,09	0,09	0,08	0,08	0,08	0,08	0,09	1
K_{CTI}		707	707	707	707	707	707	707	707	707	707	707	707	8484
$^{H}K_{CTI}$		0,09	0,08	0,08	0,08	0,08	0,09	0,09	0,08	0,08	0,08	0,08	0,09	1
K_{TF}		7	7	7	7	7	7	7	7	7	7	7	7	84
$^{H}K_{TF}$		0,09	0,08	0,08	0,08	0,08	0,09	0,09	0,08	0,08	0,08	0,08	0,09	1

Таким образом, возможен расчет оценки эффективности функционирования СЭБ на предприятии на основании реальных показателей с учетом динамики их изменения.

Кроме того, на основании предложенной методики расчета возможна автоматизация СЭБ и перевод оценки ее эффективности на автоматический процесс, т.е. реализация автоматизированной системы аудита и мониторинга функционирования СЭБ.

Список литературы

1. Кавун С.В. Информационная безопасность в бизнесе / С.В. Кавун. – Х.: ХНЭУ, 2007. – 408 с.

2. Пономаренко В. С. Концептуальні основи економічної безпеки: моногр. / В.С. Пономаренко, С.В. Кавун. – Х.: ХНЕУ, 2008. – 265 с.

3. Кавун С.В. Вопросы методики разработки системы экономической безопасности предприятия / С.В. Кавун // Вестник Международного славянского университета: український науково-теоретичний журнал. Сер. Економічні науки. – 2008. – Том XI, № 1. – С. 34 – 39.

4. Кавун С.В. Оцінка збитку організації внаслідок мережних атак на її ресурси / С.В. Кавун // Економіка розвитку. – 2007. – № 1 (41). – С. 83 – 85.