УДК 332.143 (477.54)

**Кавун С. В.**

# АНАЛИЗ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ (Г. ХАРЬКОВА И ХАРЬКОВСКОЙ ОБЛАСТИ)

*The analysis of statistical research of economic safety of the enterprises of Kharkov and the Kharkov region which are engaged in industrial or enterprise activity is offered in the article.*

*The possible variants of recommendations directed on the improvement and increasing of economic safety level of the enterprises are offered.*

В связи с развитием рыночных отношений в Украине предпринимательскую деятельность приходится осуществлять в условиях нарастающей неопределенности различных ситуаций, которые приводят к неясности и неуверенности при ведении бизнеса. Примером этому может послужить финансовый кризис этого года, который затронул экономику многих стран, в том числе и Украину.

Функционирование в условиях рыночной экономики тесно связано с рядом факторов, которые обуславливают возникновение кризисных ситуаций. Прежде всего, эти факторы порождаются непредвиденностью рыночной конъюнктуры. Поэтому привычки, приобретенные за время работы в условиях плановой экономики, теряют свою ценность, и их становится недостаточно для того, чтобы справляться с опасностями рыночной экономики. Все это приводит к необходимости проведения исследований в сфере экономической безопасности, что, в конечном итоге, должно обеспечить устранение или предвидение возникающих кризисных ситуаций (рисков), которые оказывают существенное влияние на функционирование предприятий.

Целостное понимание функционирования субъекта предпринимательской деятельности невозможно без его формализованного представления в виде экономической модели. Проведенный анализ [1; 2] позволил выявить необходимость проведения целостного исследования для субъектов предпринимательской деятельности в местном регионе, в качестве которого был выбран регион г. Харькова и Харьковской области как один из самых развитых в сфере предпринимательства (Харьковская область вошла в пятерку лидеров [3]).

Исследованиями в данной области занимались такие учене, как В. М. Геец, В. И. Мунтиян, Н. В. Куркин (Украина), Е. А. Олейников, Л. П. Гончаренко (Россия).

Кроме того, среди задач, обуславливающих необходимость проведения исследований в данном ракурсе, выделяются следующие:

1) отсутствие полной и достоверной информации об экономической безопасности (ЭБ) в сфере предпринимательской деятельности г. Харькова и Харьковской области, что связано с отсутствием каких-либо подобных исследований вообще [4];

2) присутствие случайных событий в процессе ведения бизнеса в современных рыночных условиях;

3) неформальное противостояние субъектов предпринимательской деятельности (конкуренция), что повышает актуальность учета ЭБ на предприятиях.

Таким образом, можно сформулировать цель статьи – формирование целостного представления в виде статистического анализа данных предприятий г. Харькова и Харьковской области в сфере ЭБ.

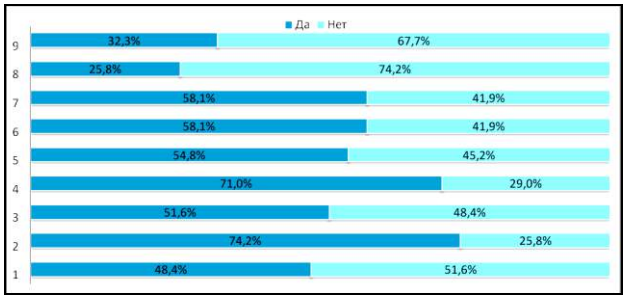
Объектом исследования являются предприятия различных форм собственности г. Харькова и Харьковской области.

Исследование проводилось методом анкетирования в течение 2-х лет в период с 2007 по 2008 год. Всего было опрошено 52 предприятия.

В принципе, представленные результаты весьма обнадеживающие, причиной этому может быть развитость самого региона (г. Харьков и Харьковская область, как известно, мощный индустриальный центр).

Примерно в половине исследованных предприятий существует выделенный отдел, со своим финансированием, со своими регламентированными юридическими документами. Их необходимость подтверждается возникающими (их не скрывают) угрозами, утечками, НСД и проводимыми вследствие этого расследованиями инцидентов. По итогам расследований на почти 60% опрошенных предприятиях была получена оценка финансовых (денежных) потерь, следовательно, руководству интересно иметь полный финансовый отчет о результатах возникновения инцидентов. Кроме того, более 2/3 исследованных предприятий считают необходимым разрабатывать и внедрять более эффективные методики оценки экономических (финансовых) потерь, следовательно, существующие методики не удовлетворяют современным требованиям рыночной экономики.

Сводная информация по общим вопросам представлена на рис. 1.




1 – существует ли в организации отдел (служба) ЭБ?
2 – существует ли положение по организации политики ЭБ в виде отдельного юридического документа?
3 – предусмотрены ли отдельные статьи расходов на ЭБ?
4 – были ли случаи сетевых (вирусных) атак, несанкционированного доступа (НСД) и т. п.?
5 – проводилось ли внутреннее расследование при возникновении утечки информации, НСД?
6 – используются ли программные средства ЭБ?
7 – оценивались ли экономические (финансовые) потери при возникновении утечки информации, НСД?
8 – нет потребности в более эффективной методике оценки экономических (финансовых) потерь при возникновении утечки информации, НСД?
9 – функции специалиста по ЭБ не выделены в отдельную должностную категорию?

Рис. 1. **Общая статистическая информация по предприятиям**

Однако, существует некоторая доля предприятий, на которых, в силу различных факторов, экономические или финансовые потери не учитываются вообще. Статистика этих причин приведена на рис. 2.

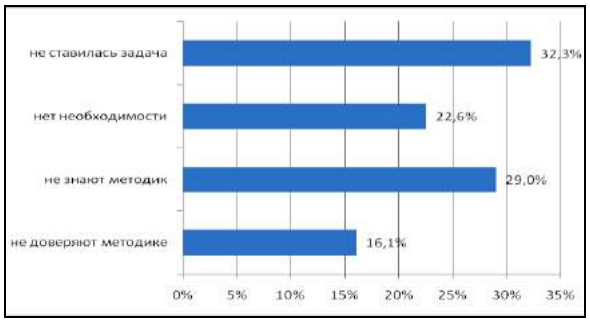



Рис. 2. **Причины отсутствия учета экономических потерь**

Несомненно, радует тот факт, что лишь на каждом восьмом предприятии умышленно не используют методики оценки ущерба, по причине недоверия им. Почти на каждом пятом предприятии считают, что в этом нет необходимости, при этом, не оговаривая сами причины.

Наличие 1/3 исследованных предприятий, на которых готовы использовать эффективные методики оценки учета экономических потерь, дает основание считать постановку данной задачи на исследование актуальной. Кроме того, одна из причин (не знание методик оценки) также подтверждает необходимость в разработке или модернизации существующих методов (методик) учета экономических или финансовых потерь. Причина, связанная с отсутствием постановки задачи учета, скорее связана либо с некомпетентностью руководства предприятия, либо с другими факторами, возможно субъективными.

Следующие статистические данные показывают аспект информационной безопасности, на котором базируется ЭБ предприятия, поскольку итоговым объектом реализации является информация. В частности на рис. 3 представлены данные, описывающие использование сканеров безопасности, которые позволяют заранее протестировать состояние отдельных элементов системы ЭБ (СЭБ).

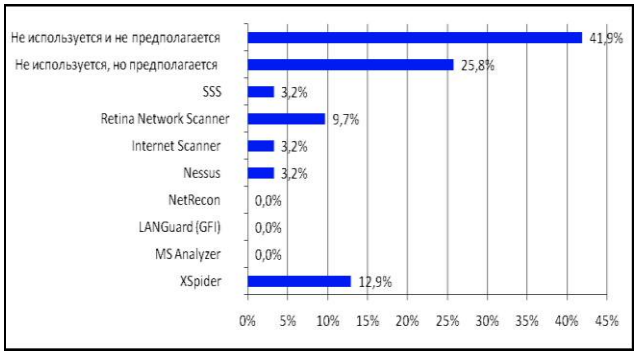



Рис. 3. **Типы сканеров безопасности, используемых на предприятиях**

Печальным фактом является отсутствие желания руководства предприятий (почти 42%) каким-то образом использовать хотя бы отдельные компоненты СЭБ, не говоря уже о целостной концепции ЭБ.

Положительная тенденция (в среднем 5% уже используют и на каждом четвертом предполагают) дает основания считать, что большая часть руководства предприятий понимают сущность реализации СЭБ.

На рис. 4 и 5 приведены результаты использования системы мониторинга (контроля) над объектами и субъектами СЭБ предприятия.

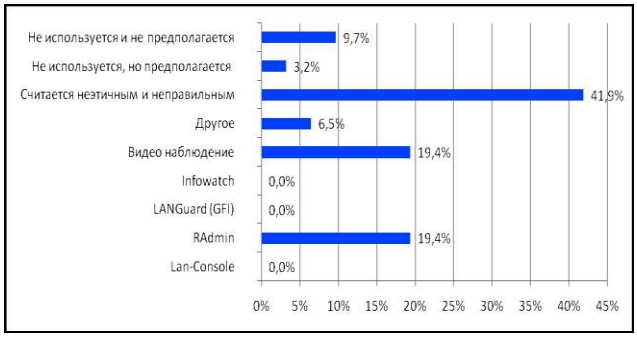



Рис. 4. **Типы используюемых средств контроля (и/или мониторинга) над действиями пользователей**

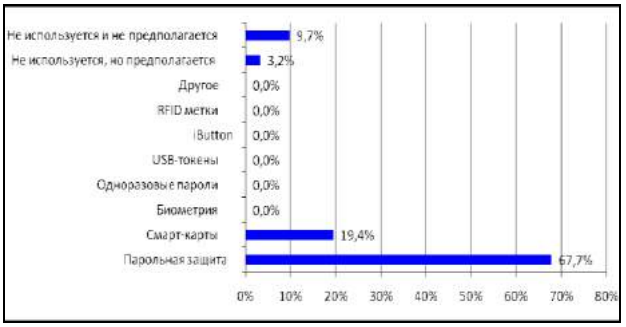



Рис. 5. **Типы используемых средств контроля доступа и аутентификации**

Как известно, ни одна реализация ИС (СЭБ) не обходится без обратной связи, которая должна подтвердить адекватность системы. Для реализации обратной связи чаще всего используется подсистема мониторинга (контроля), которая обеспечивает получение динамической статистики эффективности реализации на предприятии СЭБ в рамках общей концепции ЭБ.

В качестве подобной системы, как правило, рассматривают средства контроля над действиями пользователей, а также доступа и аутентификации.

Первый класс средств мониторинга законодательно не разрешено применять по отношению к пользователям, поскольку это влечет за собой нарушение личных прав, и, следовательно, может быть оспорено в суде. Поэтому при установке подобной системы всегда оговаривают объект мониторинга – это оборудование, различные устройства и приборы, документация, принадлежащие предприятию, и ни в коем случае это не сотрудники. Второй класс средств мониторинга необходим всегда при реализации на предприятии СЭБ для обеспечения регламентированного доступа к объектам СЭБ.

Как показало исследование (см. рис. 4) почти на каждом втором предприятии считают неэтичным использование средств первого класса. Каждое десятое предприятие в принципе не планирует их реализацию, предполагая отсутствие необходимости. Но, как показывает практика, такая необходимость возникает в самый неподходящий момент, когда наносится ущерб (экономический или финансовый). Почти на каждом пятом предприятии используется система видеонаблюдения в тандеме с системой удаленного сетевого мониторинга событий при работе на рабочей станции в сети предприятия. Безусловно, эта совокупность значительно облегчит проведение расследований фактов нанесения ущерба и позволит установить виновного.

Результаты анализа использования средств второго класса (см рис. 5) говорят, что руководство каждого десятого предприятия не планирует внедрять какие-либо системы обеспечения безопасности (в силу различных причин). Однако, почти 70% предприятий внедрили и документально обязали сотрудников (внутренние инструкции) использовать систему парольной защиты. Также было выявлено, что пока на наших предприятиях в большинстве случаев не имеют представления и современных средствах контроля доступа и аутентификации.

Поскольку каждая реализованная система (СЭБ) требует периодического контроля ее функционирования, то был также исследован аспект использования аудита ЭБ на предприятиях, результаты которого представлены на рис. 6.

Из результатов исследования видно, что почти 1/3 всех опрошенных предприятий ни разу не проводила аудит ЭБ, однако почти половина предприятий делают это регулярно. Это свидетельствует о том, что руководство этих предприятий понимают и дают объективный отчет необходимости использования на предприятии СЭБ, более того, они всячески стараются поддержать ее функционирование на должном уровне.

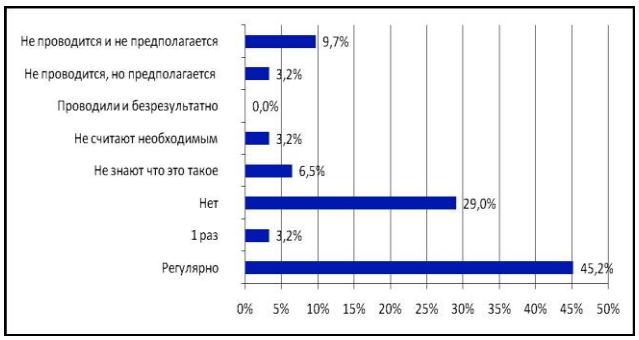



Рис. 6. **Периодичность проведения аудита ЭБ на предприятии**

Положительным является тот факт, что нет ни одного предприятия, где бы использование системы аудита не имело никаких результатов. Странным выглядит факт того, что на 6,5% предприятий вообще не имеют никакого представления о системе проведения аудита и целях его реализации. И опять же, примерно каждое десятое предприятие не имеет в своих планах проект использования аудита ЭБ на предприятии.

Каким же образом регламентируется деятельность отделов ЭБ, их сотрудников, а также соответствующих других должностных лиц? На этот вопрос отвечает полученная статистика, приведенная на рис. 7.

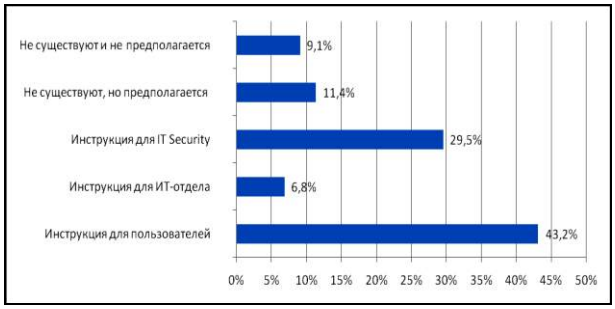



Рис. 7. **Наличие нормативных документов в области ЭБ**

Обнадеживающим фактом является то, что 4/5 предприятий имеют в своем арсенале необходимые юридические документы в виде различных инструкций специалистов и пользователей. Каждое десятое предприятие целиком понимает необходимость устранения отсутствия таковых документов, однако, каждое одиннадцатое предприятие по-прежнему и не планирует регламентирование функционирования СЭБ.

Соответственно, исходя из наличия нормативных документов в СЭБ, описываются действия персонала (почти все необходимые должностные категории), статистика которых приведена на рис. 8.

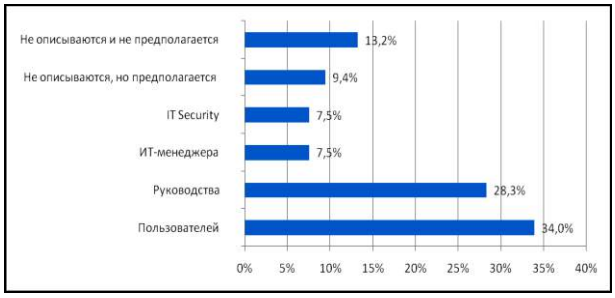
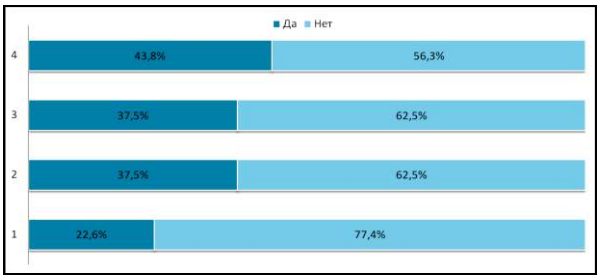



Рис. 8. **Статистика описываемых действий персонала при инцидентах**

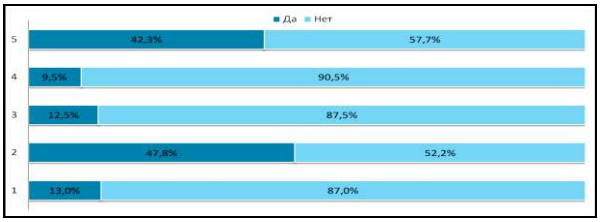
Весьма настораживающие данные по проблемам и недостаткам в ИТ-структуре предприятия приведены на рис. 9. Почти половина сотрудников считают, что ЭБ должна обеспечиваться самими сотрудниками, чуть более трети находятся в стороне от процесса функционирования СЭБ и прибыльность ставят во главе угла, забывая, что ее зависимость от результатов реализации СЭБ (ПЭБ) является прямой и линейной [6].




1 – полное отсутствие организации и структуризации
2 – прибыльность более приоритетная, чем ЭБ
3 – ЭБ важна, но это не мое дело
4 – ЭБ – дело личное каждого сотрудника

Рис. 9. **Существующие проблемы и/или недостатки в ИТ-структуре предприятия**

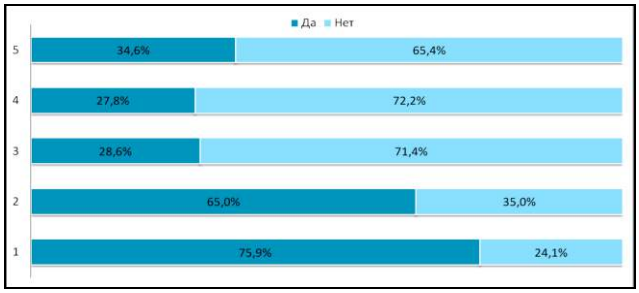
Дальнейшее исследование было посвящено защите от инсайдеров (рис. 10), из которого видно, что почти на каждом восьмом предприятии руководство доверяет своим сотрудникам и, считают, что инсайдеры [5] не представляют угрозу для них самих, причины этому могут разные, например, не смогли оценить потери, сами утечки действительно не нанесли ощутимого урона, факты утечек не были выявлены и др. Примерно половина опрошенных предприятий не имеет вообще информации о происшедших инцидентах утечек информации, конечно, это не означает, что утечек не было вообще. Настораживает то, что на каждом десятом предприятии утечки стали, своего рода, непременным атрибутом, в этом случае руководству необходимо всерьез задуматься о создании СЭБ.




1 – полное доверие своим сотрудникам
2 – нет информации об утечках
3 – инсайдеры – не угроза для предприятия
4 – часто или регулярно происходят утечки
5 – утечек нет, но они возможны

Рис. 10. **Существующие проблемы и/или недостатки в защите от инсайдеров (утечки информации внутри предприятия)**

Кто же и кому не доверяют на предприятии, показано на рис. 11.

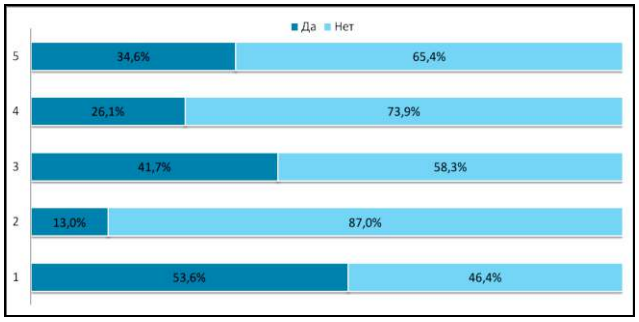



1 – вновь принятым сотрудникам
2 – собирающимся увольняться сотрудникам
3 – сотрудникам, недовольным своей зарплатой
4 – конфликтным и вспыльчивым сотрудникам
5 – все сотрудники в полном доверии

Рис. 11. **Статистика недоверия сотрудникам предприятия**

Выясняется, что в полном доверии только 1/3 всех сотрудников, а в остальных случаях неожиданностей не возникло. Как и предполагалось, недоверие выражается по отношению к недовольным, увольняющимся, кризисным в характере и т. п. [7].

Вследствие фактического недоверия возникла необходимость выявления причин проблемных ситуаций, которые складывались на предприятиях и статистика которых показана на рис. 12.

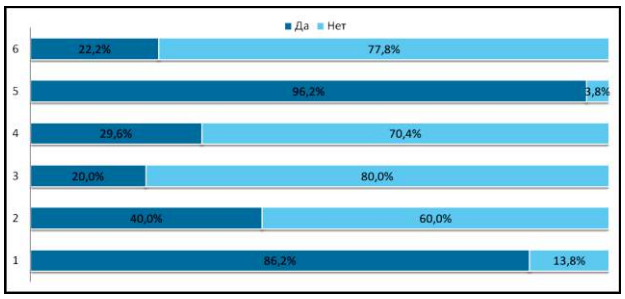



1 – недостаточная квалификация пользователей
2 – недостаточная квалификация администраторов
3 – пользователи не знают что делать и пытаются решить проблемы самостоятельно
4 – администраторы не способны расследовать инциденты и предотвращать их повторение
5 – отсутствуют правила работы и система санкций за нарушения

Рис. 12. **Причины инцидентов и проблемных ситуаций в процессе работы**

Более трети предприятий косвенно подтвердили не качественность подготовки выпускников вузов как пользователей ПК, почти половина которых, вдобавок ко всему, еще пытается самостоятельно устранить возникшую проблему. Чего нельзя сказать о профессионализме администраторов, которых, как известно, готовят специализированные вузы. То, что почти четверть администраторов не могут вести расследование и предотвращать их дальнейшее возникновение – не их вина, ввиду того, что эти решения не входят в их прямые функциональные обязанности. Для решения подобных вопросов необходимо создавать отдел ЭБ. Отсутствие правил и системы санкций является прямым следствием результатов исследований, представленных на рис. 7.

Итоговые статистические данные проведенного исследования представлены на рис. 13.




1 – сотрудники и посетители свободно перемещаются по территории
2 – действия сотрудников не контролируются и нет возможности что-либо доказать в случае возникновения инцидента
3 – сотрудник может выполнить что-либо от имени другого сотрудника
4 – сотрудники часто покидают рабочее место, оставляя ПК без присмотра
5 – сотрудники иногда используют ПК и рабочее время не по назначению
6 – сотрудники могут самостоятельно устанавливать любое ПО

Рис. 13. **Итоговые показатели исследования ЭБ на предприятиях**

Подводя итоги исследования, проведенного автором в течении двух лет, можно сказать, что для дальнейшей разработки целостной и функциональной концепции ЭБ на предприятии есть все основания.

Кроме того, факт, подтверждающий актуальность и важность проводимых исследований в сфере ЭБ предпринимательской деятельности, описывается на рис. 14, где видно, что подавляющее большинство предприятий не имеют и не знают методологий оценки функционирования СЭБ. Чуть менее половины – в виду загруженности и отсутствия больших финансовых потерь (это временно), просто не задумывались об этом. А, имея в штате грамотного юриста, руководство половины предприятий считают, что их ИС является юридически защищенной. Однако, при этом они забывают, что существует огромное количество дополнительных факторов, которые, как известно, всегда несвоевременно "подкладывают мину" в виде значительных финансовых потерь, вплоть до банкротства.


1 – юридически
2 – никогда не задумывались над этим
3 – задумывались, но не знают, как оценить

Рис. 14. **Защищенность используемой ИС от всех угроз ЭБ**

В качестве предлагаемого дальнейшего шага планирования для руководства предприятий можно предложить, с целью предупреждения возможных финансовых (экономических) потерь, уделять достаточно средств, сил и времени для разработки и реализации системы или политики ЭБ [8].

Поскольку любые статистические данные подвержены временным изменениям, то необходимо продолжать исследования по сбору и анализу данных в области ЭБ на предприятиях для получения динамической оценки реализации СЭБ и ее компонент, а также оценки эффективности ее функционирования.

---

**Литература:** 1. FBI. Computer Crime Survey. – http://houston.fbi.gov/pressrel/ 2006/ho011906.htm. 2. Кавун С. В. Информационная безопасность в бизнесе: Монография. – Харьков: Изд. ХНЭУ, 2007. – 408 с. 3. Дозор. – http://www.dozor.in.ua/node/24295. 4. Головне управління статистики у Харківській області – http://uprstat.kharkov.ukrtel.net/ua/stat/stat_inf.html. 5. Кавун С. Организация противодействия инсайдерам в предпринимательской деятельности // Економіка розвитку. – 2008. – № 1(45). – С. 9 – 11. 6. Кавун С. Методика построения политики безопасности организации / С. Кавун, Г. Шубина // Бизнес Информ. – 2005. – № 1-2. – С. 96 – 102. 7. Кавун С. Инсайдер – угроза экономической безопасности / С. Кавун, И. Сорбат // Управління розвитком. – 2008. – № 6. – С. 7 – 11. 8. Кавун С. Организационный аспект концепции экономической безопасности предприятия // Захист інформації. – 2008. – Спец. випуск № 40. – С. 113 – 119.

*Стаття надійшла до редакції 18.12.2008 р.*