

# ЭКОНОМИЧНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ РИНКОВОЇ ТРАНСФОРМАЦІЇ

УДК 658.15

**С.В. КАВУН**, канд. техн. наук, доц.

*Харьковский национальный экономический университет*

## АНАЛИЗ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Предлагается анализ состояния экономической безопасности (ЭБ) предприятия на основе статистических данных, характеризующих необходимость ее использования в рамках стратегической концепции развития предприятия. Рассматриваются различные факторы ЭБ, оказывающие существенное влияние на стратегическое развитие предприятия.

Современное развитие предприятий любых форм собственности не возможно без использования принятой концепции стратегического развития. В последнее время руководители (CEO, CSO, CISO) предприятий выделяют все больше своих активов (финансовых, технологических, временных, производственных и др.) на усовершенствование (или разработку) системы информационной безопасности, которая легко транспонируется в систему ЭБ. Это является актуальным, поскольку любой руководитель все-

гда мыслит, прежде всего, с экономической точки зрения.

Естественно, не каждый руководитель предприятия в состоянии оценить все затраты, необходимые для обеспечения функционирования системы ЭБ на заданном качественном уровне. Однако, как показывает исследование (рис.1), многие руководители понимают (это уже достаточное условие) необходимость усовершенствования ЭБ предприятия – цель данной статьи.



Рисунок 1 - Статистика решений руководителей предприятий

Полученные данные однозначно подтверждают необходимость использования системы ЭБ, которую, в конечном итоге, можно выделить в отдельную концептуальную модель концепции экономической безопасности предприятия в условиях современного развития и состояния рынка.

**Аксиома 1.** Ослабление любой составляющей инфраструктуры предприятия непосредственно отражается на его ЭБ, поэтому процесс управления предприятием должен находиться в тесной взаимосвязи с вопросами обеспечения ЭБ.

Научная новизна состоит в формировании нового подхода к экономической безопасности предприятия в концепции его стратегического развития. Данный подход

помимо известных экономических факторов предлагает учитывать также информационные и технические в комплексе, в рамках формирования концепции экономической безопасности предприятия в условиях современного развития и состояния рынка.

Также возможна и обратная связь, когда возникающие угрозы ЭБ влекут за собой заметное снижение темпов развития предприятия. Сегодня разнообразие угроз ЭБ настолько велико, что в принципе не подлежит возможной классификации, однако можно выделить основные типы, которые оказывают существенное негативное влияние (рис.2).

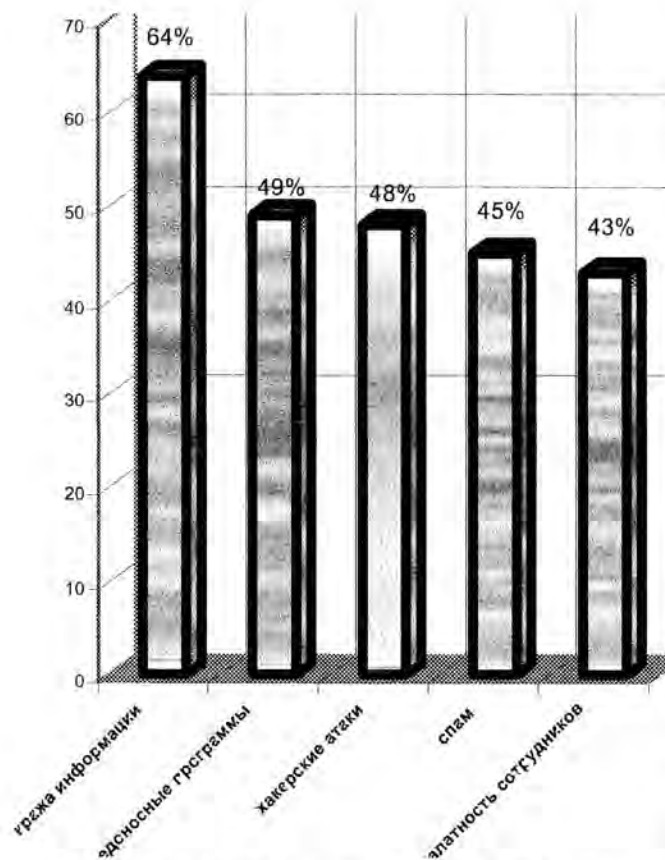


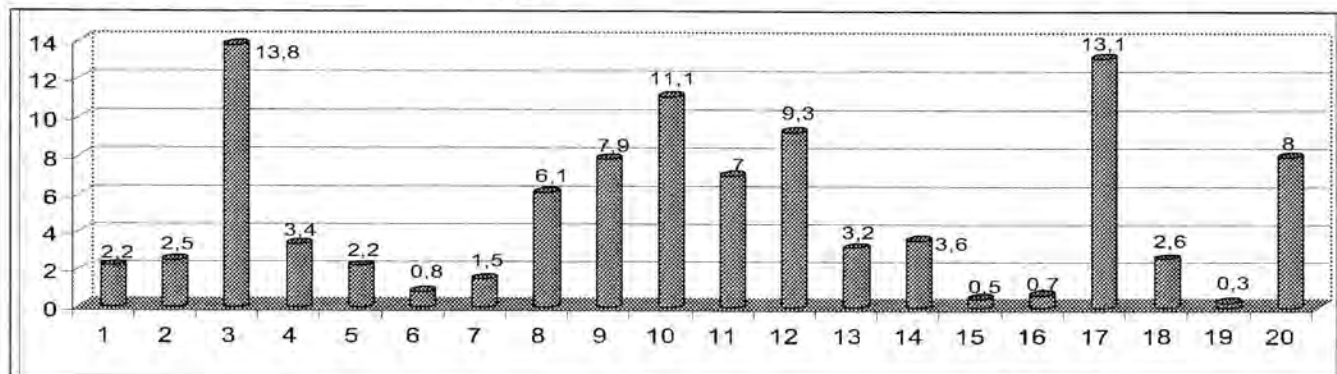
Рисунок 2 - Типы наиболее опасных угроз ЭБ

Как видно из приведенного рисунка, ранние типы угроз ЭБ (кража информации и халатность сотрудников) уже не являются лидерами в нанесении ущерба. В современном бизнесе все большее негативное влияние на концепцию развития предприятия, а, следовательно, и на ее основные экономические и финансовые показатели, оказывают современные типы угроз. В дальнейшем можно предполагать об увеличении их влияния, т.е. становится весьма актуальным вопрос о предотвращении и устранении получаемых последствий.

Все возникающие угрозы ЭБ появляются либо извне (от злоумышленников), либо исходят от своих же сотрудников, называемых в этом случае инсайдерами. Как известно, все угрозы напрямую связаны с возникающими уязвимостями в системе или организационной структуре предприятия. Вследствие проведенного аналитического исследования возможно следующее утверждение.

**Аксиома 2.** Злоумышленники достаточно медленно осваивают новые уязвимости (в виду темпа их появления), что должно быть приятно для специалистов по ЭБ. Поэтому у последних есть шанс быть на "шаг впереди" и заранее обеспечить **предотвращение** возникновения угрозы.

Проведенный анализ данных, изложенных в ежегодном отчете по компьютерным преступлениям [1] показывает сферы деятельности предприятий (рис.3).



Принятые обозначения:

1. Образование
2. Энергоносители (нефть, газ)
3. Финансы/банки
4. Государственные местные структуры
5. Государственные областные и районные структуры
6. Государственные структуры масштаба страны (включая военные)
7. Информационные технологии (аппаратное обеспечение)
8. Информационные технологии (ПО)
9. Юриспруденция
10. Здравоохранение, фармакология, биотехнология, медицина

11. Производство
12. Профессиональные и деловые услуги
13. Развлечения, торговля, розничная продажа, путешествия
14. Логистика, грузоперевозки
15. Сервис (энергетика)
16. Сервис (др.)
17. Другое
18. Бесприбыльные услуги
19. Сельское хозяйство
20. Строительство, архитектура

Рисунок 3 - Распределение сфер деятельности предприятий

Отчет был составлен на основе докладов от 2066 организаций. Из приведенных данных отчетливо видны наиболее «опасные» сферы деятельности: финансовые и банковские операции, здравоохранение, фармакология, биотехнология, медицина, сфера услуг, поскольку все они являются «денежными» с точки зрения злоумышленников.

Однако злоумышленников интересуют предприятия не только с точки зрения их финансовых и экономических успехов, а и с точки зрения масштаба самого предприятия.

Можно предположить, что на крупных предприятиях будет достаточно развитая ЭБ и, поэтому риск обнаружения существенно возрастает. Следовательно, злоумышленники будут интересоваться более мелкие предприятия, где вероятность проникновения достаточно велика, а вероятность обнаружения мала. Исследование показывает большинство предприятий, где возникают инциденты с ЭБ (рис.4), с численностью до 100 человек (по меркам Украины – это малые и средние предприятия).

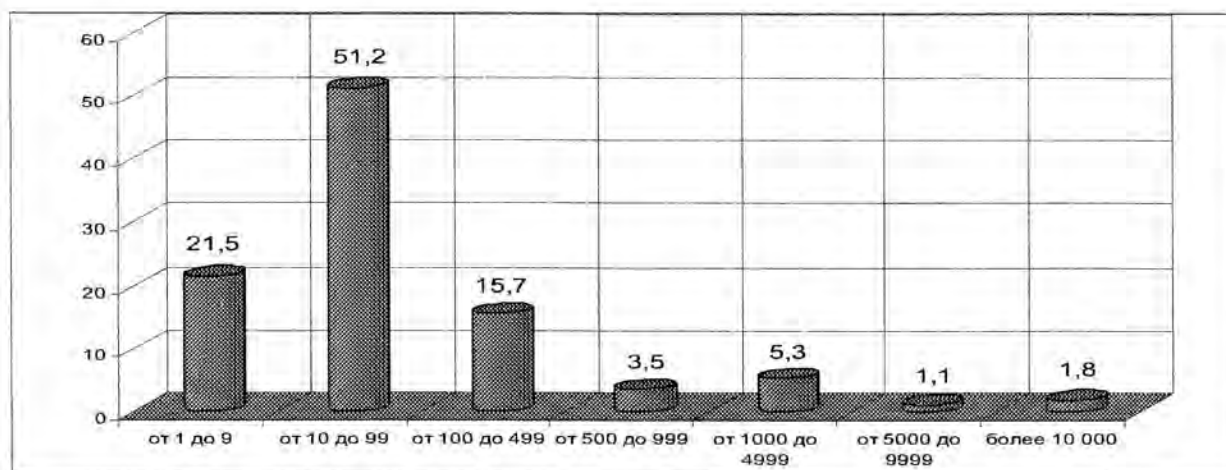
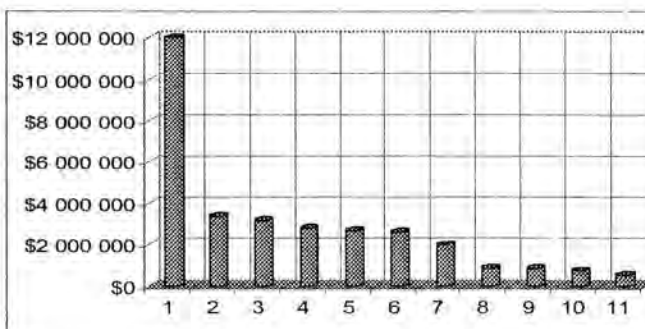
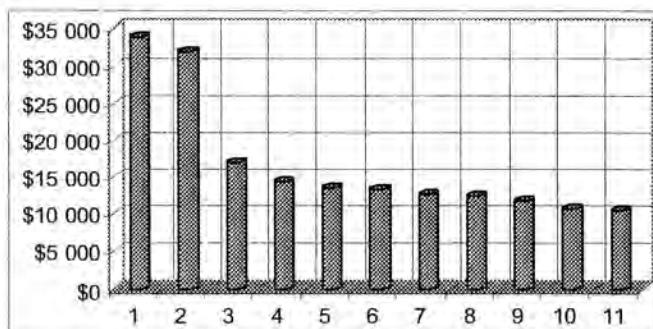


Рисунок 4 - Статистика численности сотрудников предприятий

**Аксиома 3.** Чем больше размер предприятия по численности сотрудников, тем большую цель они представляют для злоумышленников, в виду большей «напичканности» различного рода компьютерной техникой и его территориальной распределенности.

Хотя здесь надо отметить, что с увеличением размерности предприятия естественно увеличивается и его бюджет, а, следовательно, увеличиваются затраты на организацию и внедрение ЭБ, стандартизацию компьютерной техники и используемых систем защиты. Однако на большинстве предприятий на серьезную ЭБ не приходится рассчитывать, как и, собственно, на вложение достаточных финансов для повышения уровня ЭБ при ведении

современного бизнеса. Каковы же финансовые потери из-за различного типа нарушений ЭБ, выражающиеся в той или иной форме? Так как это несанкционированные воздействия, то они приводят только к потерям. Их же, как известно, всегда оценивают в денежном эквиваленте, что и является прямыми финансовыми потерями фирмы. Если же в результате таких несанкционированных воздействий фирма получает прибыль, то это уже квалифицируется как промышленный шпионаж и должно караться законными мерами. Это, разумеется, еще нужно доказать, что не всегда представляется всегда возможным. Статистика средних и суммарных потерь представлена на рис.5.



Принятые обозначения на рис. 5:

1. Вирусы (включая «черви» и троянские программы)
2. Воровство (ПК, ноутбук, КПК, ноутбуки)
3. Финансовые мошенничества
4. Сетевые атаки
5. Отказ в обслуживании (DoS, DDoS)
6. Не авторизованный доступ к организации интеллектуальной и частной

информации

7. Другие
8. Телекоммуникационные мошенничества
9. Саботаж данных или компьютерной сети
10. Неправильное использование беспроводных сетей
11. Уничтожение веб-сайтов

Рисунок 5 - Средние и суммарные потери предприятий от различного рода нарушений ЭБ

Но это все официальные данные. Автор данного исследования считает, что полученные цифры вполне можно увеличить на один, а то и два порядка, поскольку для фирмы признать факт нарушения ЭБ, да еще и признаться в финансовых потерях, — все равно, что признаться в несовершенной системе ЭБ, которая не в состоянии им противостоять. А теперь пришло время подумать об имидже этого предприятия на рынке, о доверии к ней клиентов.

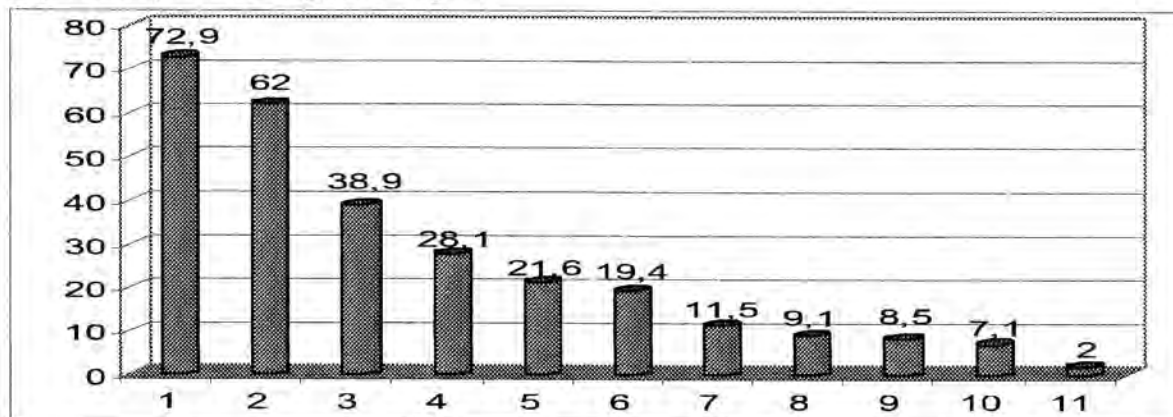
Разумным было бы принятие соответствующих мер, направленных если не на устранение возможностей потерь, то на повышение уровня ЭБ на предприятии точно. Статистический анализ типов принимаемых контрмер

повышения уровня ЭБ на предприятиях представлен на рис.6.

Многие предприятия до сих пор долго думают и колеблются при выдаче информации о нарушениях системы ЭБ, а тем более не хотят выдавать данные о финансовых потерях. Все это дает возможность сделать весьма печальный вывод: сегодня компьютерное преступление любого предприятия имеет высокую стоимость и может относиться как к индивидуальным предприятиям, так и к экономике государства в целом. Кроме того, следует также помнить, что приведенный анализ не затрагивает других типов потерь, например, человеческих, моральных, психологиче-



ских и других, которые вообще трудно измерить.



Принятые обозначения на рис. 6:  
1. Установка обновлений ЭБ на КС  
2. Установка дополнительного компьютерного ПО ЭБ  
3. Отказ в доведении информации кому бы то ни было вне фирмы  
4. Повышение уровня ПБ в корпорации  
5. Установка дополнительного компьютерного АО ЭБ  
6. Принятие дополнительных мер для идентификации злоумышленника

7. Принятие дополнительных мер для детальных контактов с ISP  
8. Доклад о компьютерных инцидентах ЭБ в специальные агентства ЭБ  
9. Предоставление право расследования инцидента ЭБ независимым внешним специалистам  
10. Другие контрмеры  
11. Сообщение о компьютерном инциденте ЭБ адвокату для возбуждения гражданского иска

Рисунок 6 - Статистика типов принимаемых контрмер

Естественным желанием после того, как выяснены понесенные потери, является желание предотвратить возможные последующие инциденты в ЭБ. Да и кто желает наступать дважды на одни и те же грабли! Разве что только весьма недалёковидный или, скажем, жадный бизнесмен, но тогда к нему применима поговорка: «Скупой платит дважды». И после всего этого пожелаем ему успехов в бизнесе.

В принципе результаты вполне очевидны: большинство использует простой путь повышения – обновление антивирусного ПО и установку дополнительного защитного ПО, что, собственно, не требует больших знаний в данной области и высокой квалификации самих пользователей. Однако примерно два из пяти предприятий не выносят информацию о возникших проблемах за пределы своего офиса, тем самым, препятствуя разглашению. То есть можно предположить, что некоторая политика ЭБ (ПЭБ) все-таки соблюдается на предприятиях.

Также можно сделать вывод, что многие предприятия все-таки имеют ПИБ [2] или ПЭБ, хотя уровень ее зрелости еще невелик, но, если судить по затратам или потерям, сами предприятия понимают всю необходимость ее усовершенствования. Каждое пятидесятое предприятие решило пойти правовым путем – нанять адвоката для решения вопроса об инциденте в свою пользу. Вывод очевиден: еще достаточное количество предприятий не доверя-

ет решение подобных проблем законным методам.

**Аксиома 4.** *Предприятия при использовании большего числа технологий и средств защиты получают больше информации о компьютерных инцидентах и, следовательно, являются более приспособленными для предотвращения, выявления и отражения атак в системе ЭБ.*

Таким образом, в современном мире при ведении бизнеса необходимо полностью отдавать отчет возможным потерям при возникновении инцидентов в ЭБ, более того, необходимо осознавать их последствия (прежде всего – финансовые). Следовательно, разумно было бы задуматься над мероприятиями, направленными на предотвращение инцидентов в ЭБ, например, начать с создания и внедрения на предприятии реально действующей ПЭБ, основанной на известных или предлагаемых методиках [3].

## ЛИТЕРАТУРА

1. FBI: Computer Crime Survey [Электронный ресурс]. – Режим доступа: [www.fbi.gov/publications](http://www.fbi.gov/publications).
2. Кавун С.В., Шубина Г.В. Методика построения политики безопасности организации // Бизнес Информ. – 2005. – № 1-2. – С.96-102.

Поступила в редколлегию 20.10.2006

## КАВУН С.В. АНАЛІЗ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Пропонується аналіз стану економічної безпеки (ЕБ) підприємства на основі статистичних даних, що характеризують необхідність її використання в рамках стратегічної концепції розвитку підприємства. Розглядаються різноманітні фактори ЕБ, які оказують істотний вплив на стратегічний розвиток підприємства.

\*\*\*

## KAVUN S.V. THE ANALYSIS OF ECONOMIC SECURITY OF THE ENTERPRISE

In article consequences the analysis of a condition of economic security (ES) the enterprises on the basis of the statistical data describing necessity of its use within the limits of the strategic concept of development of the enterprise. The various factors ES rendering essential influence on strategic development of the enterprise are considered.