УДК 658:338.45
Ілляшенко К.В., к.е.н., доцент
Таврійський державний агротехнологічний університет

# ІНФОРМАЦІЙНІ ЗАГРОЗИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

У публікації розглянуті питання впливу інформаційних технологій на економічну безпеку діяльності підприємства. Проаналізовано рівень ризиків інформаційної загрози. Запропоновані заходи щодо попередження імовірних інформаційних небезпек.
**Ключові слова:** інформація, інформаційні технології, безпека, підприємство, ризики, діяльність.

K. Ilyashenko

# INFORMATIVE THREATS ECONOMIC SECURITY OF ENTERPRISE

In a publication the questions of influence of information technologies on economic security of activity of enterprise are considered. The level of risks of informative threat is analyzed. Measures on warning of credible informative dangers are offered.
**Keywords:** information, information technologies, safety, enterprise, risks, activity.

Ильяшенко К.В.

# ИНФОРМАЦИОННЫЕ УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

В публикации рассмотрены вопросы влияния информационных технологий на экономическую безопасность деятельности предприятия. Проанализирован уровень рисков информационной угрозы. Предложены мероприятия по предупреждению вероятных информационных опасностей.
**Ключевые слова:** информация, информационные технологии, безопасность, предприятие, риски, деятельность.

**Постановка проблеми у загальному вигляді і її зв'язок з важливими науковими та практичними завданнями.** У сучасному світі інформація стає стратегічним ресурсом, одним з основних багатств економічно розвиненої держави. Швидке вдосконалювання інформатизації, проникнення її в усі сфери життєво важливих інтересів особистості, суспільства та держави викликали крім безсумнівних переваг і появу ряду суттєвих проблем. Однією з них стала необхідність захисту підприємства від імовірних інформаційних небезпек. З огляду на те, що в той час як економічний потенціал усе більшою мірою визначається рівнем розвитку інформаційної структури, пропорційно зростає потенційна уразливість економіки від інформаційних впливів.

**Аналіз останніх досліджень, у яких започатковано вирішення проблеми.** В основі дослідження питань економічної безпеки були використані роботи Шевченка І. [1], Лоханової Н.[2], Боснера Ю. [6] та інших. Вирішення проблеми інформаційної безпеки та інформаційних ризиків започатковано в працях Царєгордцева А.В. [3], Цигічка В.М. [4], Ясенєва В.М. [5] тощо. Незважаючи на велику кількість публікацій по розглянутій проблемі дотепер відсутній комплексний аналіз потенційних інформаційних загроз у діяльності підприємств.

**Цілі статті.** Метою дослідження є розгляд питання впливу інформаційних технологій на економічну безпеку діяльності підприємства, аналіз інформаційних ризиків і пошук заходів щодо попередження імовірних інформаційних небезпек.

**Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів.** Формування інформаційного суспільства опирається на новітні інформаційні, телекомунікаційні технології та технології зв'язку. Саме нові технології призвели до бурхливого поширення глобальних інформаційних мереж, що відкривають принципово нові можливості міжнародного інформаційного обміну. Формування

інформаційного суспільства концептуально та практично означає формування нового світогляду, в якому дуже важливе значення буде мати безпека від інформаційних загроз.

Інформатизація економіки розпочалася не так давно з впровадженням обчислювальної техніки та поширенням мережі Інтернет. Вона поставила ряд нових питань перед дослідниками економічної діяльності підприємств, у тому числі з питань економічної безпеки.

На даний момент можна виділити кілька поширених підходів до визначення економічної безпеки підприємства:

- захист проти економічних злочинів – забезпечення безпеки підприємства зводять до протистояння, захисту від різного роду економічних злочинів (крадіжки, шахрайство, фальсифікації, промислове шпигунство тощо). Звичайно, ці загрози дуже важливі та повинні постійно аналізуватися й ураховуватися, але зводити поняття економічної безпеки тільки до цього не можна [1, с.179];

- стан ефективного використання ресурсів або потенціалу. Підхід, що намагається уникнути вживання поняття погрози у визначенні економічної безпеки, базується на економічних поняттях досягнення мети, функціонування підприємства, тобто є ресурсно-функціональним підходом.

- наявність конкурентних переваг – підхід, послідовники якого вважають, що наявність конкурентних переваг, обумовлених відповідністю матеріальних, фінансового, кадрового, техніко-технологічного потенціалів та організаційної структури підприємства його стратегічним цілям і завданням забезпечать йому певний рівень економічної безпеки [2, с.54]. Але сам факт наявності переваг і потенціалу без їхнього використання та реалізації не гарантує підприємству економічної безпеки;

- реалізація та захист економічних інтересів – відносно новий підхід, заснований на реалізації та захисті економічних інтересів підприємства, визначає економічну безпеку як захищеність його життєво важливих інтересів від внутрішніх і зовнішніх загроз, тобто захист підприємства, його кадрового й інтелектуального потенціалу, інформації, технологій, капіталу та прибутку, що забезпечується системою мір спеціального правового, економічного, організаційного, інформаційно-технічного та соціального характеру [6, с.37].

На наш погляд, найбільш правильним є останній підхід, тому що у ньому на рівні з іншими оговорюється система мір інформаційно-технічного характеру. Але інформаційні загрози поки що не виділяються в окрему категорію.

Оскільки об'єктом інформаційної безпеки є підприємство, зміст поняття «інформаційної безпеки» буде полягати у захищеності інтересів власника даного підприємства, що задовольняють за допомогою інформації, або пов'язаних із захистом від несанкціонованого доступу тих відомостей, які представляються власникові досить важливими. Інтереси проявляються через об'єкти, здатні служити для їхнього задоволення, і дії, що вживають для володіння цими об'єктами. Відповідно інтереси як об'єкт безпеки можуть бути представлені сукупністю інформації, здатної задовольняти інтерес власника, і його дій, спрямованих на оволодіння інформацією або приховування інформації. Ці складові об'єкта інформаційної безпеки і захищаються від зовнішніх і внутрішніх погроз [3, с.54].

Зазначимо, що застосування інформаційних технологій є одним з важливих факторів, що визначають конкурентоздатність підприємств. Однак поряд з очевидними перевагами, такими як автоматизація виробничих і обліково-аналітичних процесів, доступність електронних розрахунків, швидкість обробки інформації для прийняття управлінських рішень, використання інформаційних технологій привносить нові істотні ризики [4, с. 32].

Можна привести багато визначень інформаційних ризиків, використання кожного з яких буде виправдано розв'язуваними завданнями. Саме вузьке визначення інформаційних ризиків – це ризики втрати, несанкціонованої зміни інформації через збої у функціонуванні інформаційних систем або їхнього виходу з ладу, що приводять до збитків. У цьому випадку інформаційний ризик відповідає категорії та рівню операційних ризиків у класифікації Базельського комітету "Зупинка бізнесу та збої у системах".

Найбільш широке визначення включає ризик виникнення збитків через неправильну організацію або навмисне порушення інформаційних потоків і систем організації. Таке розширене розуміння інформаційного ризику зовсім виправдано, якщо оцінювати ризики в широкому контексті інформаційної безпеки [5, с. 132].

Відповідно до базельської класифікації [7] категорій подій і прикладів дій, які можуть приводити до реалізації операційних ризиків, до інформаційних ризиків можна віднести зазначені у табл. 1.

Таблиця 1

Категорії подій і рівні інформаційних ризиків

| Рівень ризику | Категорія подій виникнення ризику | Приклади дії ризику |
|---|---|---|
| 1 | Внутрішнє шахрайство | Несанкціоноване використання інформаційних систем<br>Навмисне перекручування (приховування/розкриття) важливої інформації, що призвело до грошових втрат |
| 2 | Зовнішнє шахрайство | Незаконне проникнення в інформаційні системи, у тому числі за допомогою мережі Інтернет<br>Заподіяння збитку інформаційним системам<br>Крадіжка інформації, що призвела до грошових втрат |
| 3 | Клієнти, продукти та ведення бізнесу | Пов'язане з недостатністю систем неправомірне розкриття конфіденційної інформації |
| 4 | Збиток для матеріальних активів | Збиток матеріальним цінностям (у цьому випадку інформаційним системам) у результаті впливу зовнішніх «природних» подій<br>Збиток, що нанесено інформаційним системам від актів тероризму, вандалізму тощо |
| 5 | Зупинка бізнесу та збої у системах | Вихід з ладу інформаційних систем, окремих модулів і елементів її функціонала<br>Відмови та збої у роботі автоматизованих систем<br>Збої в роботі каналів зв'язку<br>Поломка обладнання (комп'ютери, термінали, інше встаткування) |
| 6 | Проблеми з керуванням і виконанням | Відсутність (недосконалість) системи захисту або порядку контролю доступу до інформації<br>Неправильна організація інформаційних потоків<br>Невиконання зобов'язань перед постачальниками, банками, провайдерами<br>Помилки при уведенні й обробці даних |

Можливі методи зниження для кожної одиниці інформаційного ризику стандартні для ризик-менеджменту [6, с.45]:

- прийняття ризику – визнання потенційних втрат прийнятними;
- запобігання ризику – прийняття рішень, спрямованих на видалення фактора ризику, зокрема, усунення причин відповідної погрози (наприклад, відмова від використання встановленого програмного забезпечення, що істотно порушує вимоги інформаційної безпеки);
- обмеження ризику – впровадження спеціальних засобів контролю, що знижують імовірність реалізації інформаційної загрози та (або) її наслідки;
- передача ризику – створення умов для компенсації потенційних втрат шляхом передачі ризику третій особі, наприклад, використовуючи страхування або віддаючи окремі функції на аутсорсінг.

Зазначені способи не є взаємовиключними та можуть застосовуватися комплексно.

Але запобігання інформаційним небезпекам не повинно зводитись до одного тільки зниження ризиків. Оскільки настання кризових ситуацій практично неможливо прогнозувати, необхідно створити цілу низку заходів, і перш за все, систем контролю для швидкого реагування та прийняття вірних управлінських рішень.

Проблема заслуговує більш уважного відношення від керівників підприємств, які все ще використовують застарілі моделі управління. Формування нового підходу до керування бізнес-процесами потребує перегляду кадрових питань, нових форм контролю й обов'язкового урахування факторів, що характерні новій інформаційній формі економіки.

**Висновки.** У ході дослідження нами зроблено висновок, що на даному етапі інформаційні загрози є недооціненими та недостатньо вивченими у розрізі діяльності підприємств. У той час як економічний потенціал усе більшою мірою визначається рівнем розвитку інформаційної структури, пропорційно зростає потенційна уразливість економіки від інформаційних впливів. Тому так важливо всебічно вивчити види інформаційних загроз і розробити заходи щодо їх уникнення. Це в першу чергу формування нового підходу до управління підприємством, захисту внутрішньої інформації від зовнішнього втручання, аналіз інформаційних ризиків при прийнятті управлінських рішень тощо.

Науково-технічний прогрес призвів до того, що інформаційне середовище зростає у геометричній прогресії й інформаційні технології проникають в усі сфери життя. Інформаційні аспекти економічної безпеки діяльності підприємств стають все більш пріоритетними. Таким чином, тематика інформаційних загроз економічної безпеки залишається досить актуальною, а розглянуті питання заслуговують на подальші поглиблені дослідження.

**Список використаних джерел:**


1. Шевченко І. Особливості формування економічної безпеки підприємства [Текст] / І. Шевченко // Наука молода. – 2010. – №10. – С. 178-181.
2. Лоханова Н. Система управління станом економічної безпеки підприємства: проблемні питання, концепція розвитку [Текст] / Н. Лоханова // Економіст. – 2005. – №2. – С. 52-56.
3. Царегородцев А.В. Информационная безопасность в распределенных управляющих системах: Монография [Текст] / А. В. Царегородцев. – М.: Изд-во Рос. ун-та дружбы народов, 2003. – 124 с.
4. Цыгичко В. Н. Методика оценки рисков нарушения информационной безопасности [Текст] / В. Н. Цыгичко. – М.: ИСА РАН, 2007. – 56 с.
5. Ясенев В. Н. Информационная безопасность в экономических системах: Учебное пособие [Текст] / В. Н. Ясенев. – Н. Новгород: Изд-во ННГУ, 2006. – 236 с.
6. Боснер Ю. Стратегические подходы к экономической безопасности предприятий [Текст] / Ю. Боснер // Институциональная экономика. – 2010. – №1. – С. 34-48.
7. International Convergence of Capital Measurement and Capital Standards A Revised Framework, Basel, Switzerland, November 2005.