УДК 004.056.5: 65.012.8

Нехай В.А.,
к.е.н., доцент,
доцент кафедри бухгалтерського обліку, оподаткування та аудиту,
Чернігівський національний технологічний університет
Нехай В.В.,
магістр,
аспірант кафедри інформаційних технологій та програмної інженерії,
Чернігівський національний технологічний університет

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

Анотація. У статті проаналізовано та визначено основні загрози інформаційно-комунікативній системі підприємства та їх вплив на діяльність підприємства. Наведено визначення поняття інформаційної безпеки підприємства.

Ключові слова: економічна безпека, інформаційна безпека, інформаційні технології, інформаційні системи, захист інформації.

Постановка проблеми. Н. Вінер доводив, що концептуальні схеми, які визначають поведінку біологічних систем, ідентичні до схем, які реалізуються у складних технічних системах, а отже, їх можна використовувати в соціальному та економічному управлінні, аналізувати на основі тих самих загальних положень теорії управління системами, які створені людьми [1]. Основна ідея, закладена Н. Вінером, полягає в тому, що Всесвіт складається із систем, які взаємодіють між собою на основі зворотного зв'язку. Життєздатність системи зумовлюється здатністю системи сприймати інформацію і адекватно реагувати на отриману інформацію. Мова іде про поняття стійкості системи, а отже, про здатність системи повертатися у рівноважний стан після припинення дії внутрішніх і зовнішніх збурень.

Сучасний підхід до розуміння економічної стійкості (економічної безпеки) є досить одностороннім, оскільки він обмежується рамками фінансових категорій. Під поняттям «стійкість» в економічній літературі більшість науковців та практиків розуміють здатність системи досягати своєї мети, враховуючи зміну внутрішніх та зовнішніх факторів, що приводить, як правило, до удосконалення її структурного та функціонального змісту.

У сучасних умовах господарювання особливо гостро стоїть питання обґрунтування захисту економічних інтересів українських підприємств, а також прийнятих стратегічних рішень. Євроінтеграційні процеси висувають низку вимог до підприємств України, які змушені адаптуватися до зростання рівня конкуренції та шукати адекватні рішення найскладніших проблем і шляхів зниження загроз своєї діяльності, зумовлених конфліктністю, невизначеністю та ризиками. На жаль, сучасні наукові економічні дослідження діяльності національних підприємств не дають цілісного уявлення про безпеку діяльності бізнесу. Зокрема, практично відсутнє уявлення про характер функціонування системи в агресивному середовищі та забезпечення економічної безпеки підприємства в умовах глобалізації бізнесу загалом. У нинішніх умовах господарювання постає проблема забезпечення економічної безпеки підприємств, оскільки від її вирішення залежить економічне зростання національної економіки.

Аналіз останніх досліджень і публікацій. Дослідженням питань системи економічної безпеки присвячені праці таких вчених, як П. Друкер, К. Мак-Коннел, Й. Шумпетер та ін. Система економічної безпеки досліджується у працях вітчизняних науковців, таких як О. Барановський, А. Гальчинський, Т. Клєбанова, О. Малиновська, А. Мокій, В. Шлемко. Питанням розроблення і функціонування систем захисту інформації присвячено праці В.Л. Бурячка, В.Б. Дудикевича, М.П. Карпінського, О.С. Петрова, В.О. Хорошка.

Виділення не вирішених раніше частин загальної проблеми. Стрімкий розвиток інформаційних технологій, їх застосування в управлінні діяльністю підприємств та зміна якості кібератак на інформаційні ресурси підприємства вимагає пошуку нових підходів до організації системи захисту інформаційних систем.

Метою статті є виявлення основних кіберзагроз та оцінка їх впливу на економічну безпеку підприємства, визначення можливих методів і засобів захисту від кібератак на інформаційно-комунікативну систему підприємства.

Виклад основного матеріалу дослідження. Метою забезпечення економічної безпеки підприємства має стати система протидії потенційним і реальним загрозам, розроблення превентивних заходів щодо усунення чи мінімізації яких має забезпечувати суб'єкту господарювання успішність функціонування в нестабільних умовах зовнішнього та внутрішнього середовища. При цьому безпека підприємства повинна забезпечуватися за такими основними напрямами, як економічна, науково-технічна, інформаційна, кадрова, соціальна, екологічна, фізична безпека тощо.

Прорив інформаційних технологій наприкінці XX – на початку XXI сторіччя викликав у світі значні системні перетворення, що дали можливість сформуватись і розвинутись принципово новим і невід'ємним глобальним субстанціям – інформаційному простору та інформаційному суспільству. Неконтрольоване поширення та необмежене застосування провідними країнами світу інформаційного простору як арени дій у процесі сучасного інформаційного протиборства поступово привело до уразливості інформаційної сфери цих країн до впливу внутрішніх і зовнішніх кібернетичних втручань та загроз навмисного, випадкового, природного або штучного характеру [2].

При цьому дедалі очевиднішою стає залежність загального рівня економічної безпеки держави і підприємств від її інформаційного складника.

У висновках п'ятого щорічного дослідження корпоративних ризиків «Барометр ризиків Allianz 2016» [3] зазначається,

що головним ризиком для підприємств на глобальному рівні четвертий рік поспіль залишаються перерви у виробництві і ланцюгу поставок. Однак більшість компаній стурбовані, що втрати, понесені у результаті перерв у виробництві, які зазвичай відбуваються внаслідок завдання шкоди майну, в майбутньому будуть все частіше зумовлюватися кібератаками, технічними збоями та геополітичною нестабільністю.

Стурбованість бізнесу викликає й інша глобальна сфера – це інциденти у кіберпросторі, що включають кіберзлочини або несанкціоновані втручання в бази даних, а також технічні збої в інформаційно-комунікативних системах.

Так, за даними дослідження частка кіберінцидентів зросла на 11% порівняно з 2015 роком, вперше цей ризик перемістився з п'ятої позиції на третю. Ще п'ять років тому у першому дослідженні тільки 1% респондентів розглядав кіберінциденти як ризик (табл. 1).

На жаль, менеджмент вітчизняних підприємств недостатньо приділяє уваги захисту інформаційно-комунікативних систем (табл. 2). Головними причинами є неусвідомлення можливих наслідків кібератак та значні капіталовкладення на створення системи захисту інформаційних ресурсів.

З 2011 року «Лабораторія Касперського» спільно з міжнародною аналітичною компанією B2B International проводить щорічні глобальні опитування фахівців у сфері інформаційних технологій малих, середніх і великих компаній по всьому світі.

За підсумками опитування [4] головними у сфері загроз інформаційній безпеці та протидії їм стали такі тенденції:

– 41% компаній зазначили як головний пріоритет захист конфіденційних даних від цільових атак;

– 91% компаній недооцінюють кількість існуючого шкідливого ПЗ;

– антивірусне ПЗ залишається найбільш розповсюдженим засобом забезпечення інформаційної безпеки в організаціях;

– протягом року 98% підприємств зіткнулися з інцидентами кібербезпеки, джерела яких знаходилися за межами компанії, що на 3% більше, ніж роком раніше.

– чверть компаній втратили дані в результаті зовнішніх кібератак;

– 87% компаній постраждали від внутрішніх загроз;

– чверть таких інцидентів привела до втрати конфіденційних даних;

– збиток від одного інциденту інформаційної безпеки в середньому становить близько 20 млн. рублів для великої компанії і понад 780 тис. рублів для компанії сегменту середнього та малого бізнесу;

– на ліквідацію наслідків інциденту і профілактику великі компанії додатково витрачають близько 2,1 млн. рублів, а невеликі – близько 300 тис. рублів;

– найчастіше в результаті інцидентів кібербезпеки компанії втрачають операційні дані про внутрішню діяльність, персональні дані клієнтів і фінансові відомості.

Також значні зміни відбулися у трійці найбільш пріоритетних завдань в області інформаційних технологій у порівнянні з минулим роком: головною проблемою 41% респондентів назвали захист конфіденційних даних (даних про клієнтів, фінансової інформації та ін.) від цільових атак, які в минулому році навіть не входили в цей перелік. На друге місце (34%) перемістилося більш загальне питання захисту даних, яке лідиру-

Таблиця 1

Найбільш значимі ризики для підприємств Європи*

№	Ризики	Рейтинг 2016 р.	Місце в рейтингу 2015 р.
1	Перерва у виробництві та постачанні	53%	1
2	Ринкові зміни (волатильність, посилення конкуренції, стагнація)	52%	нове
3	Кіберінциденти (кіберзлочини, витік даних, збої IT)	40%	5
4	Зміни в законодавстві та регулюванні (економічні санкції, протекціонізм)	39%	4
5	Макроекономічні зміни (жорстка економія, зростання цін, інфляція)	31%	нове
6	Природні катастрофи (гроза, повінь, землетрус)	31%	2
7	Втрата репутації або вартості бренду	29%	7
8	Пожежа, вибух	22%	3
9	Нові технології та інновації	19%	нове
10	Політичні ризики (війна, тероризм, заворушення)	17%	8

**Рейтинг складений експертами Редакції Форіншурер http://forinsurer.com/news/16/01/28/33453*

Таблиця 2

Найбільш значимі ризики для підприємств України*

№	Ризики	Рейтинг 2016 р.	Місце в рейтингу 2015 р.
1	Політичні ризики (війна, тероризм, заворушення)	65%	1
2	Розкрадання, шахрайство і корупція	39%	2
3	Тероризм	35%	4
4	Пожежа, вибух	27%	3
5	Перерва у виробництві та постачанні	23%	5
6	Природні катастрофи	15%	7
7	Макроекономічні зміни (жорстка економія, зростання цін, інфляція)	15%	8
8	Єдиний соціальний внесок ринку	15%	9
9	Кіберінциденти (кібератаки, витік даних, збої IT)	15%	нове
10	Зміни в законодавстві та регулюванні (протекціонізм)	12%	10

**Рейтинг складений експертами Редакції Форіншурер http://forinsurer.com/news/16/01/28/33453*

вало до цього протягом трьох років. А третє місце отримало завдання, яке раніше теж не потрапляло в список пріоритетних – 29% опитаних відзначили необхідність забезпечення безперебійної роботи критично важливих систем (наприклад, за рахунок застосування засобів захисту від DDoS-атак).

Тому невипадково питання інформаційної безпеки вже давно входить до числа головних пріоритетів менеджменту всіх великих національних і світових компаній, а останніми роками все більше число керівників середнього і малого вітчизняного бізнесу починають усвідомлювати реальну небезпеку ризиків, пов'язаних з інсайдерською інформацією.

Можливість зовнішнього і внутрішнього втручання в інформаційну систему підприємства може вплинути на викривлення таких параметрів інформації, як конфіденційність, цілісність, доступність, достовірність та ін. Це може привести до негативних наслідків у діяльності підприємства:

– збоїв у функціонуванні систем управління технологічними та управлінськими процесами;

– розголошення відомостей, що становлять комерційну та інші види таємниць;

– порушення достовірності фінансової звітності;

– несанкціонованого доступу до бази даних підприємства;

– викривлення публічної інформації тощо.

Результатом викривлення інформації про діяльність підприємства можуть стати:

– зменшення вартості капіталу підприємства;

– труднощі залучення інвестицій;

– розрив (або погіршення) ділових відносин із партнерами;

– зрив переговорів, втрата вигідних контрактів;

– невиконання договірних зобов'язань;

– відмова від рішень, які стали неефективними через розголос інформації;

– втрата можливості запатентувати результат науково-технічної діяльності або продати ліцензію;

– зниження цін або обсягів реалізації;

– нанесення шкоди авторитету та діловій репутації фірми;

– більш жорсткі умови отримання кредитів;

– труднощі в постачанні та придбанні устаткування тощо.

У певних ситуаціях нехтування питаннями захисту інформації може привести і до повної втрати бізнесу.

Поняття інформаційної безпеки можна розглядати у декількох аспектах. По-перше, це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави. По-друге, це стан захищеності потреб в інформації особи, суспільства і держави, за якого забезпечується їх існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.

Науковцями термін «інформаційна безпека» розуміється по-різному, причому найчастіше мається на увазі якийсь один аспект цієї проблеми (табл. 3). На нашу думку, інформаційна безпека підприємства полягає у формуванні принципів, методів та заходів щодо виявлення, аналізу, запобігання та нейтралізації негативних джерел, причин і умов впливу на інформацію.

При цьому поняття «інформаційна безпека» характеризує стан інформаційного захисту господарюючого суб'єкта в умовах, коли існує імовірність загроз, що досягається системою заходів, спрямованих на попередження, виявлення та ліквідацію інформаційних загроз.

Таким чином, спектр інтересів інформаційної безпеки щодо інформації, інформаційних систем та інформаційних технологій як об'єктів безпеки можна поділити на такі основні категорії, як доступність – можливість за визначений час отримати певну інформаційну послугу; цілісність – релевантність та несуперечливість інформації, її захищеність від руйнування та несанкціонованого змінювання; конфіденційність – захищеність від несанкціонованого доступу.

З позиції інформаційних технологій захисту інформації інформаційна безпека – це система заходів, що дає змогу виявляти вразливі місця інформаційно-комунікативної системи підприємства, небезпеки, які загрожують їй, і методи нейтралізації виявлених загроз.

Загрозою визнається подія, яка може викликати порушення функціонування інформаційної системи, включаючи спотворення, знищення або несанкціоноване використання бази даних.

Можливість реалізації загроз залежить від наявності вразливих місць в інформаційній системі. Склад і специфіка вразливих місць визначається типом вирішуваних завдань, характером інформації, апаратно-програмними особливостями обробки інформації на підприємстві, наявністю засобів захисту та їхніми характеристиками.

Таблиця 3

Визначення поняття «інформаційна безпека» науковцями

Автор	Визначення
Хоффман Л. Дж. [5]	інформаційна безпека – це стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації
Литвиненко О. [6]	під інформаційною безпекою варто розуміти одну зі сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами
Горбатюк О.М. [7]	інформаційна безпека являє собою стан захищеності потреб в інформації особистості, суспільства і держави, за якого забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз
Богуш В. [8]	інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави
Сороківська О. [9]	під інформаційною безпекою підприємства пропонуємо розуміти суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності
Бурячок В.Л. [2]	кібербезпеку можна визначити як стан захищеності кіберпростору держави загалом або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам

Теорія та практика свідчить про існування двох груп загроз щодо інформаційної безпеки підприємства, таких як ненавмисні або випадкові дії, що виражаються в неадекватній підтримці механізмів захисту та помилках в управлінні, та навмисні загрози – несанкціонований доступ до інформації і несанкціонована маніпуляція даними, ресурсами і самими системами.

Також класифікація загроз інформаційній безпеці може бути здійснена поділом загроз на пов'язані із внутрішніми і зовнішніми факторами.

Окремо варто виділити загрози, пов'язані з навмисними помилками, що виникають за межами бізнесу. До таких загроз відносять [2, 10]:

– несанкціонований доступ до інформації, що зберігається в системі;

– заперечення дій, пов'язаних із маніпулюванням інформацією (наприклад, несанкціонована модифікація, яка веде до порушення цілісності даних);

– введення в програмні продукти і проекти «логічних бомб», які спрацьовують за виконання певних умов або після закінчення певного періоду часу і частково або повністю виводять з ладу комп'ютерну систему;

– розроблення і поширення комп'ютерних вірусів;

– недбалість у розробленні, підтримці та експлуатації програмного забезпечення, що приводить до краху комп'ютерної системи;

– зміна комп'ютерної інформації і підробка електронних підписів;

– розкрадання інформації з подальшим маскуванням;

– перехоплення інформаційних потоків;

– заперечення дій або послуги;

– відмова в наданні послуги.

На жаль, доводиться констатувати, що уніфікований підхід до класифікації загроз інформаційній безпеці відсутній. І це цілком зрозуміло, тому що при всьому тому різноманітті інформаційних систем, спрямованих на автоматизацію безлічі технологічних процесів, які зачіпають різні сфери людської діяльності, жорстка систематизація та класифікація загроз неприйнятна. Дослідивши джерела [2, 10], можна запропонувати таку класифікацію загроз:

– За проявом та наслідками – злочин; шахрайство; хуліганство.

– За типом – програмне; апаратне, інше.

– За метою – оперативні, тактичні, стратегічні.

– За характером виникнення – навмисні, ненавмисні.

– За інформаційними технологіями – об'єкт загроз, методи підготовки загроз, інструментарій загроз, середовище загроз.

– За місцем виникнення – інсайдерські, зовнішні.

– За об'єктом впливу – системні, локальні.

– За причиною виникнення – збої в обладнанні, збої в роботі програмного забезпечення, недосконала архівація даних, несанкціонований доступ.

Розвиток інформаційних технологій та засобів комунікацій забезпечують все більш широкі можливості доступу до інформаційних ресурсів та переміщення великих масивів даних на необмежені відстані. При цьому доступ широкого кола користувачів, місце знаходження яких може бути довільним, до ресурсів, що знаходяться будь-де у межах глобальної інформаційної мережі, збільшує загрозу інформаційним ресурсам підприємства й інформаційній системі підприємства загалом. Тому інформація як продукт, що має попит, потребує збереження та надійного захисту.

Висновки. Одним із найважливіших видів діяльності із забезпечення інформаційної безпеки підприємства є виявлення, оцінка та запобігання загрозам інформаційно-комунікативним системам і інформаційним ресурсам. Сучасна корпоративна система інформаційної безпеки покликана забезпечувати захист конфіденційної інформації від несанкціонованого доступу, запобігати зловмисним або випадковим змінам (контролювати цілісність) і давати необхідний рівень доступу. Забезпечення інформаційної безпеки зводиться до трьох основних напрямів – це комбінація технічних, адміністративних і організаційних заходів.

Таким чином, у сучасних умовах господарювання, коли інформаційні технології набувають глобального характеру, інформаційна безпека є невід'ємним складником системи економічної безпеки господарюючого суб'єкта й економічної безпеки держави загалом.

Література:

1. Виннер Н. Кибернетика и общество / Н. Виннер. – Издательство иностранной литературы. Москва, 1958. – 200 с.
2. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби [Підручник] / В.Л. Бурячок, Г.М Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
3. Top 10 Global Business Risks for 2016: [Електронний ресурс]. – Режим доступу: http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer 2016.pdf
4. Информационная безопасность бизнеса 2014: [Електронний ресурс]. – Режим доступу: http://media.kaspersky.com/pdf/IT_risk_report_Russia_ 2014.pdf
5. Хоффман Л. Дж. Современные методы защиты информации / Л. Дж. Хоффман [пер. с англ.]. – М: Советское радио, 1980. – 57 с.
6. Литвиненко О. Інформація і безпека / О. Литвиненко // Нова політика. – 1998. – № 1. – С. 47–49.
7. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О.М. Горбатюк // Вісник Київського університету імені Т. Шевченка. – 1999. – Вип. 14: Міжнародні відносини. – С. 46–48.
8. Богуш В. Інформаційна безпека держави/ В. Богуш, О. Юдін; [Гол. ред. Ю.О. Шпак]. – К.: «МК-Прес», 2005. – 432 с.
9. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко // Економічні науки: Вісник Хмельницького національного університету 2010. – № 2. – Т. 2. – С. 32–35.
10. Литвинов В.В. Моделювання та аналіз безпеки розподілених інформаційних систем: навч. пос. [для студ. спец. 121 «Інженерія програмного забезпечення»] / В.В. Литвинов, В.В. Казимир, І.В. Стеценко та ін. – Чернігів: Чернігів. нац. технол. ун-т, 2016. – 254 с.

Нехай В.А., Нехай В.В. Информационная безопасность как составляющая экономической безопасности предприятий

Аннотация. В статье проанализированы и определены основные угрозы информационно-коммуникативной системе предприятия и их влияние на деятельность предприятия. Приведено определение понятия информационной безопасности предприятия.

Ключевые слова: экономическая безопасность, информационная безопасность, информационные технологии, информационные системы, защита информации.

Nekhai V.A., Nekhai V.V. Information security as a constituent of economic security

Summary. The article analyses and defines the main threats to the information and communication system of an enterprise and their impact on the activities of the enterprise. The definition of information security of the enterprise is given.

Keywords: economic security, information security, information technology, information systems, data protection.