Максим ТАНЦЮРА

АНАЛІЗ ІНФОРМАЦІЙНИХ ЗАГРОЗ ТУРИСТИЧНИХ ПІДПРИЄМСТВ АР КРИМ

Стаття присвячена питанням аналізу інформаційних загроз туристичних підприємств АРК. Автор розглядає основні види внутрішніх та зовнішніх інформаційних загроз, їх причини та динаміку. Особлива увага приділяється кадровим та програмним загрозам як основному джерелу інформаційних збитків туристичних підприємств АРК.

Ключові слова: *аналіз, інформація, загрози, туристичні підприємства, АРК.*

Аналіз інформаційних загроз туристичних підприємств є необхідною передумовою для побудови ефективної системи їхньої інформаційної безпеки. Метою аналізу є превенція деструктивного впливу несприятливих факторів середовища функціонування підприємства на інформаційні ресурси та інфраструктуру. Основним завданнями аналізу є визначення причин, джерел та видів інформаційних загроз, оцінення вірогідності та наслідків реалізації інформаційних загроз.

Окремі аспекти аналізу інформаційних загроз відображені у *працях вітчизняних та зарубіжних науковців*. Економічні та правові аспекти інформаційних загроз досліджували *такі вчені*: І. В. Арістова, А. Бонакорси, П. Гиури, А. Г. Горшенков, Ф. Пьеротти та ін. Технічні та соціальні аспекти інформаційних загроз досліджували О. Воробйова, Р. А. Калюжний, П. П. Маслянко, О. Г. Найдьонов, В. С. Цимбалюк та ін. Водночас в економічній літературі відсутній комплексний підхід до аналізу інформаційних загроз туристичних підприємств АР Крим.

Метою даної статті є формування та використання комплексного підходу до аналізу інформаційних загроз туристичних підприємств АР Крим.

З огляду на вивчення літературних джерел (табл. 1) причини виникнення інформаційних загроз ми можемо розділити на зовнішні, на які не може впливати окреме підприємство, та внутрішні, які залежать безпосередньо від конкретного підприємства. Безумовно, вказаний поділ загроз має умовний характер, бо часто на практиці доволі важко відокремити внутрішні загрози від зовнішніх.

Таблиця 1

Основні зовнішні причини виникнення інформаційних загроз на туристичних підприємствах

Групи	Причини
Економічні [1, 2, 3]	– зростання значення інформації як бізнес-ресурсу; – розвиток інформаційного ринку; – здешевлення доступу до інформаційних мереж та потужної обчислювальної техніки;
Правові [4, 5, 6]	– недосконалість правової бази у галузі інформаційної безпеки; – складність виявлення та розслідування інформаційних правопорушень;
Технічні [7, 8, 9]	– збільшення обсягів інформаційного обміну через технічні канали; – поширення автоматизації та інформатизації діяльності підприємств; – створення централізованих баз даних;
Соціальні [10, 11, 12]	– підвищення рівня інформаційної грамотності населення; – непопулярність норм інформаційної етики.

Аналізуючи табл. 1, можемо зробити висновок, що зовнішні причини виникнення інформаційних загроз можна поділити на дві основні групи.

Перша група зовнішніх причин – це об'єктивні тенденції суспільного розвитку. До них належать: зростання значення інформаційних ресурсів, розвиток інформаційного ринку, підвищення інформаційної грамотності населення, здешевлення доступу до інформаційних мереж та обчислювальної техніки, збільшення обсягів інформаційного обміну, інформатизація. Ці тенденції мають глобальний характер, окрема держава не може впливати на них. Завдання підприємства, яке прагне забезпечувати належний рівень своєї інформаційної безпеки, полягає в тому, щоб простежувати та вивчати динаміку цих процесів для своєчасної адаптації до змін зовнішнього середовища.

Друга група зовнішніх причин – це недоліки державного регулювання та рівня культурного розвитку населення. До них належать: недосконалість правової бази, складність виявлення та розслідування інформаційних правопорушень, непопулярність норм інформаційної етики. Ці проблеми є побічним ефектом пришвидшення темпів інформатизації. Їхнє вирішення є одним із пріоритетних завдань державних органів, які відповідають за проведення інформаційної політики.

Проаналізуємо внутрішні причини інформаційних загроз на основі узагальнення результатів анонімного анкетування співробітників туристичних підприємств. У табл. 2 наведено основні внутрішні причини загроз, на які вказали респонденти, та відносна кількість опитуваних, що вказали відповідний варіант.

Таблиця 2

Внутрішні причини виникнення інформаційних загроз туристичних підприємств АР Крим*

Причини	Відносна кількість респондентів, %
– нерозуміння зв'язку між інформаційною безпекою та проблемами підприємницької діяльності;	19,3
– ігнорування проблем інформаційної безпеки;	17,1
– делегування повноважень щодо забезпечення інформацією співробітників, які не мають відповідної кваліфікації;	15,9
– недооцінка вартості інформації та репутації підприємства;	13,6
– використання реактивних короткострокових заходів, які не вирішують проблему до кінця;	11,5
– використання окремих засобів безпеки без забезпечення їхньої комплексності;	8,4
– відсутність належного контролю за виконанням рішень з інформаційної безпеки;	7,6
– інші причини	2,9

*За даними опитування.

Як видно з табл. 2, можна виокремити сім основних причин виникнення інформаційних загроз туристичних підприємств АР Крим. Найбільша кількість респондентів зазначила, що саме нерозуміння зв'язку між інформаційною безпекою та проблемами підприємницької діяльності є основною причиною проблем інформаційної безпеки.

Дані за джерелами інформаційних загроз представлені у табл. 3.

Таблиця 3

Джерела інформаційних загроз туристичних підприємств АРК*

Джерела	Кількість інцидентів, %				
	2005 р.	2006 р.	2007 р.	2008 р.	2009 р.
Природні фактори	2,1	2,3	2,1	2,2	2,3
Антропогенні загрози	42	44,1	49,2	55,1	59,9
у т. ч.:					
– співробітники підприємства	31,2	32,4	35,1	38,7	41,4
– пов'язані із підприємством особи, що не є співробітниками	9,1	10,1	12,3	14,5	16,7
– сторонні особи	1,7	1,6	1,8	1,9	1,8
Технічні загрози	55,9	53,6	48,7	42,7	37,8
у т. ч.:					
– апаратні загрози	31,8	28,1	19,6	11,6	3,6
– програмні загрози	7,3	8,4	10,6	11,2	12,9
– мережеві загрози	16,8	17,1	18,5	19,9	21,3

*За даними опитування.

З даних табл. 3 видно, що джерела інформаційних загроз діляться на три групи:

а) природні – вплив факторів навколишнього середовища;

б) антропогенні – дії чи бездіяльність людини (групи людей);

в) технічні – використання апаратного та/або програмного забезпечення.

Суб'єктами антропогенних загроз можуть бути:

– наймані працівники підприємства, у т. ч. звільнені з роботи;

– пов'язані із підприємством особи (клієнти, конкуренти та контрагенти);

– державні службовці, які проводять адміністративний контроль за діяльністю підприємства;

– особи, які не мають прямого відношення до діяльності підприємства;

Аналізуючи дані за останні п'ять років, бачимо, що кількість інцидентів, що трапляється у результаті дії природних факторів, суттєво не змінюється. Відсутня також чітка тенденція у даних щодо інформаційних загроз, джерелом яких є сторонні особи.

Водночас чіткі тенденції до зростання демонструють антропогенні загрози, джерелом яких є співробітники підприємства (загальний приріст – 10,2% інцидентів) та інші пов'язані особи (загальний приріст – 7,6% інцидентів), що пов'язано зі збільшенням питомої ваги працівників, які зайняті інтелектуальною працею та зростанням кількості клієнтів.

Технічні загрози демонструють чітку тенденцію до зниження (загальне зменшення – 18,1% інцидентів), хоча за окремими видами технічних загроз динаміка відрізняється: за програмними та мережевими загрозами спостерігається відчутне збільшення кількості інцидентів, а за апаратними – зменшення, що зумовлено наступними обставинами:

– здешевлення обчислювального обладнання;

– інтелектуалізація процесу обробки інформації;

– підвищення кількості інформації, що передається за технічними каналами зв'язку;

– збільшення обсягу онлайн-послуг та онлайн-транзакцій.

За станом на 2009 р. найменша кількість інцидентів (1,8%) пов'язана із сторонніми особами, а основним джерелом інформаційний загроз є співробітники підприємства (41,4% інцидентів). У зв'язку з цим необхідно більш детально проаналізувати причини кадрових загроз (рис. 1).

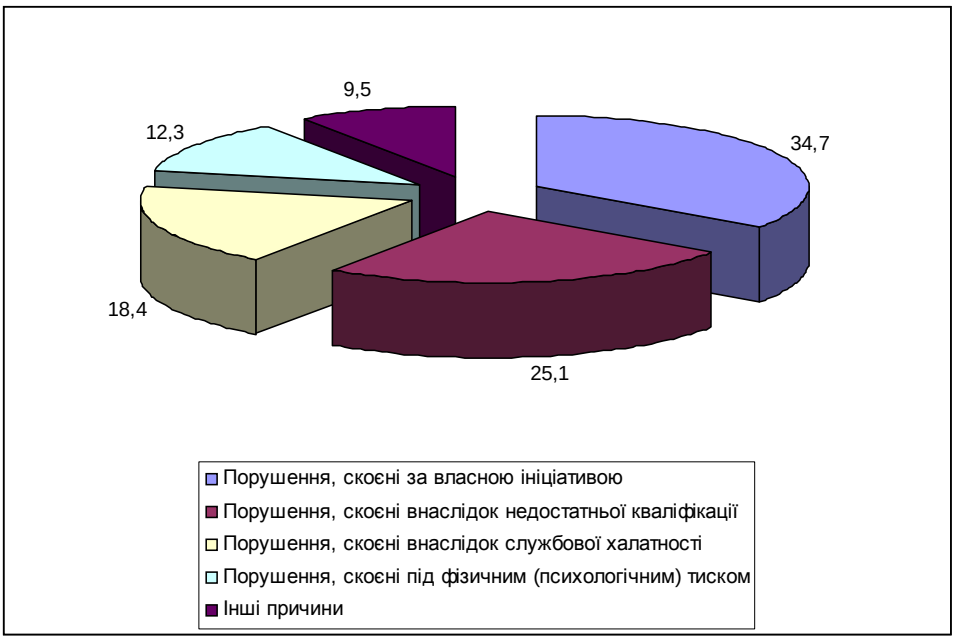

Рис. 1. ***Причини кадрових загроз інформаційної безпеки у 2009 р.***

З огляду на дані вищенаведеної діаграми ми можемо розділити основні причини кадрових загроз на дві групи:

1) навмисні дії (бездіяльність), коли суб'єкт передбачає можливі негативні наслідки своїх дій, вони можуть виконуватись із власної ініціативи або унаслідок фізичного чи психологічного тиску;

2) ненавмисні дії (бездіяльність), які виконуються внаслідок недостатнього рівня освітньої підготовки працівників у галузі інформаційних технологій або недбалого ставлення до виконання службових обов'язків.

Відповідно до даних табл. 3, доволі значним є також рівень технічних загроз, існування яких пов'язано з використанням автоматизованих систем для організації інформаційних процесів, їх можна розділити на три основні групи:

1) апаратні – пов'язані з використанням спеціального обладнання для зберігання та обробки інформації;

2) програмні – пов'язані з використанням спеціального програмного забезпечення для обробки інформації;

3) мережеві – пов'язані з процесом передачі інформації через технічні канали зв'язку.

Під апаратними маються на увазі такі загрози: 1) несанкціоноване втручання у діяльність технічних засобів; 2) порушення правил використання технічних засобів; 3) відмови техніки (поломки, помилки і т. п.); 4) порушення режиму енергопостачання та інші.

Програмні загрози реалізуються у формі помилок, які виникають у процесі функціонування програмного забезпечення, та деструктивних програм. Комп'ютерні

програми, що спеціально розробленні для здійснення інформаційних правопорушень (malware), вважаємо, за метою функціонування можна поділити на такі групи:

1) інфекційні (їхня мета – пошкодження даних та обладнання):

– комп'ютерні віруси – програми, які мають такі властивості: здатність несанкціонованого проникнення в інші програми; самостійне розповсюдження у комп'ютерній системі; спрямованість на пошкодження даних;

– черви – вони відрізняються від вірусів лише тим, що існують незалежно від існуючих на комп'ютері програм;

– експлойти – це програми, які використовують вразливості захисту програм для вчинення з їхньою допомогою несанкціонованих дій;

2) шпигунські програми (spyware) (їх мета – несанкціоноване отримання конфіденційної інформації):

– трояни – це програми, які проникають у комп'ютер під виглядом корисного для користувача додатка, але виконують після проникнення також несанкціоновані та непрофільні дії;

– руткіти (rootkit) – це набір програмних засобів для несанкціонованого адміністрування інформаційної системи;

– бекдори (backdoor) – це програми, за допомогою яких виконується обхід передбаченої у системі процедури аутентифікації;

– кілогери (keyloggers) – програми несанкціонованого знімання інформації, що вводиться в інформаційну систему за допомогою клавіатури;

3) паразитарні (їхня мета – несанкціоноване використання обчислювальної потужності стороннього комп'ютера);

4) рекламні програми (adware) та спам; – їхня мета – поширення інформації про продукти та послуги без попереднього замовлення через індивідуальні канали інформації (електронну пошту, комунікаційні програми і т. п.). Небезпечність спаму полягає у тому, що він підвищує рівень надлишкової інформації, відволікає співробітників та ресурси на виконання непродуктивних дій.

Динаміка кількості шкідливих програм за 2005–2009 рр. наведена на рис. 2. Як бачимо з вищенаведеної діаграми, кількість шкідливих програм за останні п'ять років постійно зростає: у 2006 р. порівняно з попереднім роком кількість шкідливих програм збільшилася у 2,86 разу, у 2007 р. – у 2,64 разу, у 2008 р. – у 7,09 разу, у 2009 р. – 1,81 разу. Швидкість цього зростання не є постійною, що відображає зусилля спеціалістів з інформаційної безпеки по боротьбі зі шкідливими програмами. Значна зміна ланцюгового темпу зростання у 2008 р. зумовлена впливом світової фінансової кризи.

Аналізуючи дані туристичних підприємств, можемо зробити висновок, що внутрішні загрози, пов'язані з інформаційними ресурсами підприємства, існують у формі порушення цілісності інформації, витік інформації, недоступність інформації, а зовнішні, пов'язані із зовнішнім інформаційним полем підприємства, – у формі дезінформації; інформаційної асиметрії; "інформаційного шуму".

Під дезінформацією розуміється отримання підприємством неправдивої інформації або поширення неправдивої інформації про підприємство. Базуючись на неправдивій інформації підприємець ризикує прийняти нераціональне рішення, що знизить ефективність управління. Поширення неправдивих та негативних відомостей про підприємство може призвести до погіршення ділової репутації та втрати клієнтів.

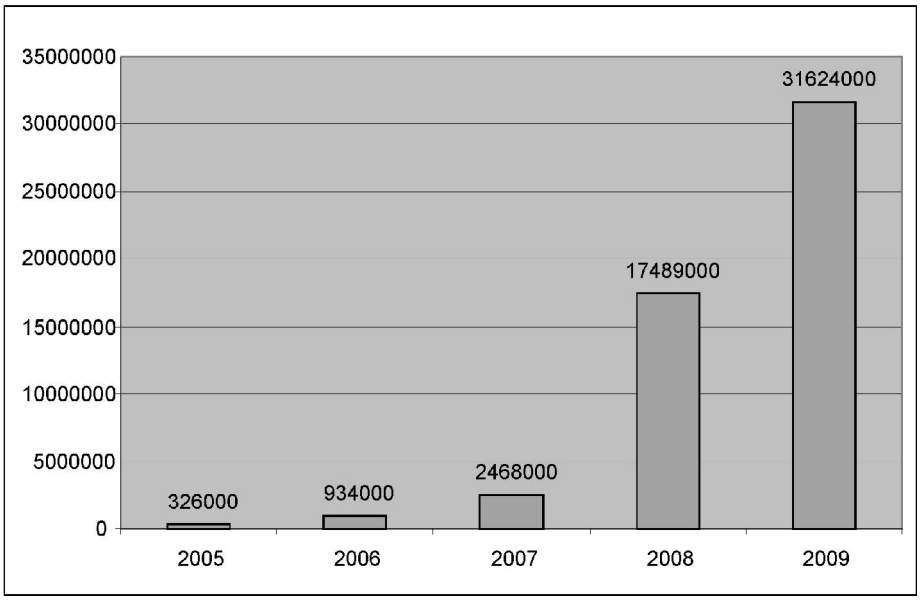

Рис. 2. *Динаміка кількості шкідливих програм**

*За даними ЗАО "Лабораторія Касперського"

Поняття "інформаційна асиметрія" ("інформаційна нерівність") на глобальному рівні було вперше використано у 1997 р. ООН [13]. Під інформаційною нерівністю (асиметрією) розуміють ситуацію, коли кількість та/або якість інформації, що є у розпорядженні кожного із суб'єктів суспільних відносин, відрізняється або змінюється непропорційно. Подібна ситуація може бути наслідком нерівності можливостей доступу до інформаційних ресурсів та інформаційно-комунікаційної техніки.

"Інформаційний шум" характеризує ситуацію, коли підприємство отримує інформацію, яка в нього вже є або яка йому не потрібна. У зв'язку з пришвидшенням темпів збільшення обсягів інформації у світі проблема надлишковості інформації постійно загострюється, що вимагає від підприємства постійного вдосконалення методів збору, аналізу та зберігання даних, а також придбання інноваційної техніки.

Отже, бачимо, що зовнішні загрози доволі суттєво, хоча й непрямо, впливають на діяльність туристичних підприємств. З огляду на те, що трансформувати їх індивідуально майже неможливо, необхідно проводити детальний моніторинг з метою вчасної адаптації до найменших змін кон'юнктури. Водночас не менш *важливим завданням* є вивчення та реагування на існування внутрішніх причин виникнення інформаційних загроз, що може стати предметом подальшого дослідження.

Література

1. *Using Knowledge Management to Drive Innovation. – American Productivity & Quality Center, 2003. – 194 p.*
2. *Влияние сектора информационных технологий на национальную экономику и перспективы создания "электронного правительства" // Информационный бюллетень Microsoft "Государство в 21 веке". – 2002. – Вып. 15. – С. 1–50.*

3. *Bonaccorsi A., Giuri P., Pierotti F. Technological strategies and market success. Evidence from the aero-engine Industry // Journal of Business Ven-turing, 2002. Vol. 17. – P.24–40.*
4. *Крылов В. В. Информационные компьютерные преступления. – М.: Инфра-М – Норма, 1997. – 285 с.*
5. *Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти: Монограф. / За заг. ред. д-ра юрид. наук, проф. О. М. Бандурки. – Харків: Вид-во Ун-ту внутр. справ, 2000. – 368 с.*
6. *Горшенков А. Г., Горшенков Г. Г., Горшенков Г. Н. Информационная преступность: криминологическая безопасность личности, угрозы и меры ее защиты // Вестник Нижегородского университета им. Н. И. Лобачевского. Сер.: "Право". – 2003. – № 1. – С. 13–16.*
7. *Воробйова О. Інформаційне суспільство та його вплив на становлення електронного бізнесу // Науковий вісник. – 2010. – Вип. 5. – С. 1–9.*
8. *Маслянко П. П. Концепція інформатизації корпоративних структур // Наукові вісті НТУУ "КПІ". – 2003. – № 3. – С. 510–525.*
9. *Антопольский А. Б. Вопросы интеграции информационных ресурсов и структура информационного пространства // Технологии информационного общества – Интернет и современное общество: VI Всероссийская объединенная конференція (Санкт-Петербург, 3–6 ноября 2003 г.) – СПб.: Изд-во Филологического ф-та СПбГУ, 2003. – С. 42–43.*
10. *Найдьонов О. Г. Інформатизація як головна ідея третього тисячоліття // Ученые записки Таврического национального университета им. В. И. Вернадского. – Сер. "Философия. Культурология. Политология. Социология". – 2010. – Т. 23 (62), № 2. – С. 161–165.*
11. *Інформаційне суспільство: Дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція / [В. М. Брижко, О. М. Гальченко, В. С. Цимбалюк та ін.]. – К.: Інтеграл, 2002. – 220 с.*
12. *Інформатизація управління соціальними системами: Організаційно-правові питання теорії і практики: Навч. посіб. / [Д. Гавловський, Р. А. Калюжний, В. С. Цимбалюк та ін.]. – К.: МАУП, 2003. – 332 с.*
13. *К обществам знания: Всемирный доклад ЮНЕСКО. – Париж: ЮНЕСКО, 2005. – 231 с.*

Редакція отримала матеріал 18 березня 2011 р.