Електронне наукове фахове видання "Ефективна економіка" включено до переліку наукових фахових видань України з питань економіки (Наказ Міністерства освіти і науки України від 29.12.2014 № 1528)

Ефективна ЕКОНОМІКА

Дніпропетровський державний аграрно-економічний університет

№ 3, 2016 Назад Головна

УДК 658.012.8:343.46

Н. О. Бабіна,
к. е. н., доцент кафедри економіки,
Київський національний університет технологій та дизайну, м. Київ

РЕЙДЕРСТВО ЯК ЗАГРОЗА ЕКОНОМІЧНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

N. O. Babina,
Ph.D. in Economics, Assistant Professor, Department of Economics,
Kyiv National University of Technologies and Design

RAIDING AS A THREAT TO ECONOMIC SECURITY OF ENTERPRISE

Рейдерство є суттєвою загрозою для економічної безпеки сучасного українського суспільства як на рівні господарюючих суб'єктів, так і на рівні національної безпеки країни. В розвинених країнах рейдерство є ефективним важелем впливу на неефективні підприємства. В Україні рейдерство виступає, перш за все, знаряддям перерозподілу власності та реалізації особистих інтересів. Загострення боротьби за право володіти бізнесом чи контролювати його актуалізується в період зміни влади, посилення правової, організаційної та економічної нестабільності в країні.

Серед низки ознак, що сигналізують про привабливість підприємства для рейдерів, першорядною є збір економічної, юридичної та соціальної інформації про компанію.

Для отримання необхідної інформації рейдерами широко використовується промислове шпигунство. Ефективними способами одержання інформації, що містить комерційну таємницю, є підкуп співробітників підприємства, шантаж, влаштування «своїх» людей до складу персоналу підприємства-конкурента та переманювання провідних спеціалістів організації.

Рейдери не тільки аналітично обробляють отриману інформацію, але й самі активно моделюють проблемні ситуації та розповсюджують неправдиву інформацію про господарюючого суб'єкта, чим шкодять його іміджу.

Збереження конфіденційної інформації, забезпечення нейтралізації загроз рейдерських атак можливо лише за умови правильно організованої та адаптованої до сучасної трансформаційної економіки системи економічної безпеки підприємства, в якій інформаційна складова займає провідне місце.

Raiding is an obvious threat to the economic security of present-day Ukrainian society, either at the level of economic entities or national security. In the developed countries raiding is an effective leverage of influence onto non-effective enterprise. In Ukraine raiding is first and foremost a means of proprietorship taking over/redistribution and gaining personal interests. The exacerbation of internecine wars for business control or propriety rights is felt painfully in the period of power shifting, legal, managerial and economic instability in the country.

One of the markers for raiding appeal is accumulation of economic, legal and social information about the company.

To get the desired information an industrial espionage is widely used. Other effective means of information leakage are bribing, blackmailing, insiders and luring of top professionals in the company- competitor.

Raiders not only analytically process the obtained info, they also construe and simulate the problem situations and spread the misleading information about the economic entity thus undermining its image and reputation.

Confidential info securing as well as eliminating raiding attacks is feasible only under the conditions of effectively organized and adapted to the present-day transforming economy system of economic security of enterprise. Information is an integral and most prominent element of it.

Ключові слова: *трансформаційна економіка, рейдерство, загроза, безпека, економічна безпека, інформаційна безпека.*

Keywords: *transformation economy, raiding, threat, security, economic security, information security.*

Постановка проблеми. Однією з актуальних проблем трансформаційної економіки України є рейдерство. Від нього потерпають як промислові підприємства, так і організації невиробничої сфери, суб'єкти малого та середнього бізнесу.

До зовнішніх чинників, що «підживлюють» рейдерство можна віднести пролонговану економічну кризу (що призвела до безлічі фінансово-економічних небезпек підприємницької діяльності і загроз для бізнесу в цілому); розширення «сірого» сектору економіки; складність соціально-політичної ситуації в країні (особливо в умовах війни на сході); недосконаліть комерційного законодавства; криміналізацію суспільства; неефективну протидію корупції. Зниження фінансово-господарських показників діяльності підприємств; збільшення кредиторської заборгованості; відсутність корпоративного духу і схильність персоналу до шахрайства та розголошення комерційної таємниці за винагороду є тими внутрішніми чинниками, які сприяють активізації рейдерських атак.

Аналіз останніх досліджень і публікацій. Значний внесок в дослідження проблеми рейдерства зробили Б.Андрушків (антирейдерство, економічна та майнова безпека підприємства і підприємництва), Т.Бабич (рейдерство як загроза національній безпеці), О.Бєліков (рейдерство в Україні), П.Берназ (визначення поняття рейдерства, його специфіка в Україні), З.Варналій (передумови та шляхи подолання рейдерства в Україні), С.Васильчик (рейдерство, як ознака хвороби економіки), О.Дічек (правові ознаки рейдерства та шляхи його запобігання), З.Живко (особливості рейдерства в ринковій економіці), Д.Зеркалов (міжнародна та національна безпека під кутом зору рейдерства), К.Каліцінська (ризики, пов'язані з рейдерством), М.Колєсник (тенденції розвитку рейдерства в Україні),

Л.Нечипоренко (інтелектуальні аспекти рейдерства), Н.Олексюк (методи захисту від корпоративного рейдерства), Н.Приймак (рейдерство в сучасній економіці України), Н.Яковенко (рейдерство як специфічний феномен) та ін.

Проте дана тема залишається актуальною внаслідок виникнення в практиці трансформаційної економіки різноманітних економічних аномалій, новітніх загроз і «викликів» часу. Недостатньо вивченими є превентивні технології протидії протиправному перерозподілу прав власності; сучасні методи і інструменти управління ризиком рейдерства, його впливу на економічну безпеку підприємства; роль різноманітних інститутів в протидії рейдерським акціями, в тому числі і виконання державою функції координації конкуренції в масштабах національного господарства.

Мета статті. Дослідити можливі шляхи мінімізації ризику рейдерства для економічної безпеки підприємства під кутом зору практичних викликів суперечливої трансформаційної економіки України.

Виклад основного матеріалу. З рейдерством суб'єкти підприємницької діяльності України зіткнулися вже на початку 90-х рр. XX століття, коли на фоні політичної нестабільності, прогалин в законодавстві, наявності тіньового сектору активно ішов процес протиправного перерозподілу прав власності. Час від часу, в період зміни влади, посилення правової, організаційної та економічної нестабільності відбувається загострення боротьби за право володіти бізнесом чи контролювати його.

Об'єктом рейдерських атак може стати будь-який бізнес, в незалежності від його активів, результатів господарської діяльності, галузевої та регіональної приналежності. Суб'єктами рейдерства можуть виступати стейкхолдери, фізичні та юридичні особи, конкурентні організації, кредитні організації, страхові компанії, органи державної та місцевої влади, засоби масової інформації.

Рейдером на заході називають компанію, яка поглинає інші компанії, скуповуючи акції компанії-жертви з метою отримання її контрольного пакету; а рейдерством - як звичайне і абсолютно законне придбання організації без згоди фактичного власника і менеджменту, так і силове захоплення з метою зміни власника [1].

Зарубіжні дослідники ринків корпоративного контролю провідних країн світу (К. Мілхауф, В. Шверт, А. Шлейфер, Р. Вішни, С. Клейзенс, Дж. Фан) пропонують досить потужні методи та системи ризик-захисту від недружніх поглинань. Проте, слід зауважити, що західні превентивні заходи зорієнтовані на акціонерні товариства, діють у виваженому законодавчому полі і розраховані на законний перерозподіл прав власності. Тому впровадження зарубіжних методів і систем ризик-захисту суб'єктів господарювання від рейдерських атак потребує адаптації до специфічної трансформаційної економіки України.

Серед низки ознак, що сигналізують про привабливість підприємства для рейдерів, першорядною є збір економічної, юридичної та соціальної інформації про компанію. Рейдерів цікавлять: (1) документи (засновницькі, приватизаційні, внутрішні (положення, регламенти), про активи підприємства, його боргові зобов'язання та ін.); (2) інформація (про ринкову позицію підприємства; його соціальну політику; про близькість менеджменту до адмінресурсу; про судові позови і рішення щодо працівників підприємства, звільнених раніше, зокрема); (3) чутки (про конфлікти на підприємстві, особливо між власниками, керівництвом та підлеглими; про приватне життя топ-менеджерів та інших ключових осіб, від яких залежить ефективна діяльність підприємства).

Рейдери не тільки аналітично обробляють отриману інформацію, але й самі можуть активно моделювати та втілювати ситуації, що шкодитимуть економічній, фінансовій, кадровій та інтерфейсній політиці господарюючого суб'єкта.

За даними експертів в Україні нараховується до 50 професійних рейдерських груп, що об'єднують досвідчених економістів, юристів, психологів, IT-технологів та ін. Розповсюджуючи в засобах масової інформації неправдиву негативну інформацію про підприємство; ініціюючи перевірки контролюючими органами; використовуючи підкуп менеджерів та силових структур, підробку документів, психологічний тиск, шантаж підприємства (через тактику гринмейлу, зокрема) чи його співробітників, вони формують умови рейдерських атак, захоплення і перерозподіл власності, спираючись на законодавство, яке не може миттєво реагувати на виклики багато в чому непередбачуваних трансформаційних процесів. Відтак, щорічний обсяг рейдерського перерозподілу власності в Україні сягає в середньому від 2 до 3 млрд. дол. США [2, с. 2].

Для протидії загрозі рейдерства підприємство має приділити увагу переформатуванню своєї системи економічної безпеки і, в першу чергу, забезпечити збереження конфіденційної інформації як у внутрішньому середовищі, так і неможливість її витоку від контрагентів чи партнерів по бізнесу.

В сучасній ринковій економіці у рази підвищилась інтенсивність інформаційно-комунікаційних процесів, характерною рисою яких є широке впровадження і використання інформаційних технологій. Разом з позитивними можна констатувати збільшення негативних явищ, безпосередньо пов'язаних з використанням інформації, інформаційних продуктів і послуг. Зростання правопорушень у сфері електронного документообігу, збільшення несанкціонованих доступів до інформації та навмисне спотворення її змісту, ріст обману та шахрайства спонукає дослідників визначати стан інформаційної сфери, як «інформаційну війну» [3].

Для успішного функціонування системи інформаційної безпеки підприємства, перш за все, необхідно визначити коло найбільш вірогідних загроз для суб'єкта господарювання і оцінити рівень їх актуалізації; виявити та скласти карту-схему найбільш вразливих місць в інформаційній системі, постійно їх моніторити; розробити систему заходів профілактики та мінімізації збитків, що спричинені інформаційним продуктам, ресурсам, інформаційній інфраструктури суб'єкта в цілому. Особливо підкреслимо, що при створенні системи інформаційної безпеки підприємство має врахувати свої специфічні особливості інформаційної взаємодії з іншими суб'єктами ринку, серед яких провідне місце займають: конкурентоздатність продукції на внутрішніх і зовнішніх ринках; інноваційний рівень техніки і технологій; практика спілкування з контрагентами на основі Internet-технологій; укладання угод та реалізація продукції за допомогою використання E-commerce [4].

Заходи із забезпечення інформаційної безпеки, з однієї сторони, спрямовані на охорону конфіденційної інформації (запобігання несанкціонованому доступу до локальних комп'ютерних мереж, усунення «жучків» та ін.); з іншої - включають контрзаходи (пошук, обробка і використання інформації про конкурентів, партнерів, контрагентів), які підтримують розвиток підприємства і є базою відвертання небезпек.

Для отримання необхідної інформації рейдерами широко використовується промислове (підприємницьке) шпигунство. Для підприємницького шпигунства інтерес становить саме конфіденційна інформація, яка відноситься до комерційної таємниці, є цінною, оскільки приносить прибуток чи надає підприємству переваги у будь-якій сфері [5].

Сьогодні протистояти підприємницькому шпигунству стає дедалі складніше: у складній політичній і соціально-економічній ситуації для країни легше використовувати неадаптованість законодавства до сучасного етапу розвитку суспільства; знайти і фінансово зацікавити «розвідників» високої степені кваліфікації, озброєних сучасною технікою; виявити прогалини в системі економічної безпеки підприємства, яка потребує постійних грошових вливань для удосконалення, щоб якісно відповідати на непередбачувані загрози.

До новітніх загроз економічній безпеці підприємства слід віднести професіоналізацію кримінального світу, який не поступається «чистому» бізнесу в сфері отримання корисної інформації про стратегічні й тактичні наміри конкурентів з метою здобуття конкурентної переваги на ринку через витіснення або знищення суперника; проте при рейдерських атаках використовує перевірені практикою прямі загрози менеджменту підприємства чи членам їх родини та силове захоплення.

Суб'єктами підприємницького шпигунства, як правило, є особи, які (або за допомогою яких) реалізують зовнішні загрози інформаційній безпеці господарюючих суб'єктів: конкуренти, агенти конкурентів, злочинні елементи, партнери, а також суб'єкти, що не зв'язані з підприємницькою діяльністю та ін. До специфічної категорії суб'єктів підприємницького шпигунства відноситься персонал, який реалізує внутрішні загрози інформаційній безпеці підприємства. Тому на підприємстві повинна бути встановлена система, яка забезпечує передачу конкретним особам тільки такого обсягу інформації, який дозволяє їм сумлінно виконувати свої службові обов'язки і знижує рівень можливих збитків при переході працівника до фірми-конкурента.

Рейдери постійно працюють з особами, які мають допуск до комерційної таємниці, використовують підкуп, шантаж, дружнє спілкування. Отримавши доступ на підприємство, можуть незаконно проникнути в комп'ютерну мережу підприємства, викрасти важливу документацію, встановити апаратуру для прослуховування телефонних розмов.

Найбільш простим і ефективним способом одержання комерційної таємниці є підкуп співробітників підприємства долучених до потрібної інформації. Тому об'єктами рейдерської уваги стають співробітники, які незадоволені своїм заробітком, кар'єрним зростанням, характером відносин з керівництвом, ті, хто гостро потребує грошей та ін. Досить розповсюдженими методами отримання секретної інформації залишається шантаж, влаштування «своїх» людей до складу персоналу підприємства-конкурента та переманювання провідних спеціалістів організації. Останнє дозволяє не тільки отримати у значному обсязі потрібну інформацію, але й ослабити конкурента, зробити його вразливим до рейдерських атак.

Сьогодні у виграшній позиції знаходяться суб'єкти, що провадять інформацію, виробляють інформаційні продукти і послуги, спираючись на властивості інформації, визначають рівень її цінності та продукують системи її захисту від небажаних небезпек. Тому сучасні підприємства для ефективної інформаційної безпеки своєї діяльності все частіше створюють інформаційно-аналітичний підрозділ служби безпеки, що забезпечує втілення інформаційної складової економічної безпеки підприємства, має на меті досягнення належного рівня інформаційної безпеки шляхом прогнозування тенденцій розвитку науки і технологій, дотичних до процесів діяльності підприємства; моніторинг інформаційного простору всередині і поза межами підприємства за для отримання інформації, що стосується життєво важливих для підприємства процесів, її аналізу і оптимального використання; захист конфіденційної інформації [6].

Для створення ефективної системи інформаційної безпеки підприємства необхідно: визначити та контролювати ймовірні канали витоку інформації на підприємстві; постійно контролювати доступ співробітників до корпоративних інформаційних ресурсів, посадовими інструкціями встановити рівень доступу лише до тієї інформації, яка потрібна для роботи; обов'язково зберігати архів операцій з документами, архівувати поштову кореспонденцію; моніторити вихідний потік електронних повідомлень, які можуть нести загрозу витоку таємної інформації; здійснювати моніторинг на рівні файлових операцій; контролювати використання мобільних пристроїв зберігання інформації, пристроїв передачі інформації і комунікативних портів; правильно підібрати кадри, застосовуючи матеріальні та моральні стимули; утвердження сприятливого соціально-психологічного клімату всередині підприємства, створення можливостей для професійного росту персоналу, сприяння зниженню плинності кадрів, формуванню «фірмового патріотизму».

Бажаний результат можна отримати лише при своєчасному та комплексному виконанню цих завдань.

Активне протистояння рейдерству можливе за реалізації низки факторів: від вдосконалення чинного корпоративного законодавства та об'єднання зусиль силових структур до широкої участі громадськості та ЗМІ у боротьбі з протиправним перерозподілом прав власності. [7]. Але завчасне передбачення та попередження рейдерських атак, як реальної загрози економічній безпеці підприємства, є більш ефективним та фінансово вигідним шляхом вирішення означеної проблеми, ніж боротьба з наслідками від конкретних рейдерських дій.

Важливим превентивним заходом протидії протиправному перерозподілу прав власності є правильно організована та адаптована до сучасної ринкової економіки система економічної безпеки підприємства, в якій інформаційна складова займає провідне місце, як найбільш мобільна та відкрита до інноваційних викликів трансформаційної економіки.

Подальшого дослідження потребує роль інших складових системи економічної безпеки підприємства у виявленні, локалізації і протистоянні загрозам рейдерських атак.

Висновки.

В сучасному українському суспільстві рейдерство є суттєвою загрозою для економічної безпеки як на рівні господарюючих суб'єктів, так і на рівні національної безпеки країни.

В розвинених країнах рейдерство є дійовим інструментом впливу на неефективні підприємства, в Україні, перш за все, - виступає знаряддям перерозподілу власності та досягнення особистих інтересів. Загострення боротьби за право володіти бізнесом чи контролювати його актуалізується в період зміни влади, посилення правової, організаційної та економічної нестабільності в країні.

Серед низки ознак, що сигналізують про привабливість підприємства для рейдерів, першорядною є збір економічної, юридичної та соціальної інформації про компанію. Для отримання необхідної інформації рейдерами широко використовується промислове шпигунство, для якого найбільш цінною є інформація, що становить комерційну таємницю. Ефективними способами одержання необхідної інформації є підкуп співробітників підприємства, шантаж, влаштування «своїх» людей до складу персоналу підприємства-конкурента та переманювання провідних спеціалістів організації.

Тільки правильно організована та адаптована до сучасної ринкової економіки система економічної безпеки підприємства може не тільки не допустити витоку конфіденційної інформації, але й забезпечити нейтралізацію загрози рейдерських атак через силову, фінансову, кадрову, інтерфейсну та ін. складові.

Література.

1. Савельєв Є. В. Економічна та майнова безпека підприємства і підприємництва. Антирейдерство/ Є. В. Савельєв, З. В.Гуцайлюк, В. В. Козюк та ін. // Тернопіль: Вид. Терно–граф, 2008. - 424 с.

2. Бабич Т. Рейдерство в Україні – загроза національній безпеці / Т. Бабич // Віче. – 2010. – № 14. – С. 2-5.

3. Прокоф'єва Д. М. Підприємницьке шпигунство в системі інформаційних злочинів / Д. М. Прокоф'єва //Український центр інформаційної безпеки. Режим доступу: www.bezpeka.com/library/lib_aspect.html.

4. Янчева Л. М. Електронна комерція: організація та облік: навчальний посібник / Л. М. Янчева, А. П. Грінько, А. С. Крутова, Т. О. Тарасова // Харків: ХДУХТ, 2008. - 231 с.

5. Бабіна Н.О. Сучасні технології захисту комерційної таємниці від промислового шпіонажу / Н.О.Бабіна// Вісник КНУТД. – 2010. - №5 (5). – С.13-18.

6. Babina N.O. Challenges in ensuring information security for Ukrainian business in modern economic milieu/ Н.А.Бабина// Международное научное издание «Современные фундаментальные и прикладне исследования». – 2013. - №2(9). – С.53-55.

7. Варналій З. С., Мазур І. І. Рейдерство в Україні: передумови та шляхи подолання / З. С. Варналій, І. І. Мазур // Стратегічні пріоритети. – 2007. – № 2 (3). – С. 129-139.

References.

1. Savelyev, Ye. V. Hutsailyuk, Z. V. and Kozyuk, V. V. (2008), *Ekonomichna ta mainova bezpeka pidpryyemstva i pidpryyemnytstva. Antyreiderstvo* [Economic and property security of enterprise and business], Terno–graf, Ternopil, Ukraine.

2. Babych, T. (2010), "Raiding in Ukraine as a threat to national security", *Viche,* vol. 10, pp. 2–5.

3. The official site of Ukrainian Center of Information Security (2016), "Economic espionage in the system of information crimes", available at: www.bezpeka.com/library/lib_aspect.html (Accessed 17 February 2016).

4. Yancheva, L. M. Hrinko, A. P., Krutova, A. S. and Tarasova, T. O. (2008), *Elektronna komerciya: orhanizaciya ta oblik.* [eCommerce: structure and accounting process], KHDUKHT, Kharkiv, Ukraine.

5. Babina, N. O. (2010), "Modern technologies of trade secret protection from industrial espionage", *Visnyk KNUTD,* vol. 5 (5), pp. 13–18.

6. Babina, N.O. (2013), "Challenges in ensuring information security for Ukrainian business in modern economic milieu", *Sovremennyye fundamentalnyye i prikladnyye issledovaniya, vol.*2(9), pp. 53–55.

7. Varnaliy, Z. S. and Mazur, I.I. (2007), "Raiding in Ukraine: prerequisites and ways of overcoming", *Stratehichni priorytety*, vol. 2(3), pp. 129–139.

Стаття надійшла до редакції 18.03.2016 р.