DOI: https://doi.org/10.32782/2524-0072/2019-20-28

УДК 65.012.8

Інформаційна безпека підприємств в умовах глобалізації 4.0

Дейнега Олександр Вікторович
кандидат економічних наук, доцент,
проректор з наукової роботи
Рівненського державного гуманітарного університету

Deineha Oleksandr
Rivne State Humanitarian University

Ідентифіковано цінність захисту інформації для підприємств різних масштабів. Конкретизовано зміст поняття «культура захисту інформації» у системі управління підприємством. Виявлено проблеми у сфері захисту інформації вітчизняних підприємств. Досліджено відмінності у підходах до реалізації заходів із забезпечення захисту інформації промисловими підприємствами різного масштабу на ринку B2B. Виокремлено чинники, що визначають кількісний і якісний склад способів і прийомів захисту інформації. Розкрито суть та умови реалізації принципу економічної доцільності захисту інформації. Проаналізовано причини та наслідки втрат підприємств у результаті витоку інформації. Визначено відмінності у підходах до оцінювання втрат від витоку інформації промисловими підприємствами різного масштабу на ринку B2B.

Ключові слова: інформація, захист інформації, промислові підприємства, економічна доцільність захисту інформації, втрати від витоку інформації.

Дейнега А.В. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЙ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ 4.0.

Идентифицирована ценность защиты информации для предприятий различных масштабов. Конкретизировано содержание понятия «культура защиты информации» в системе управления предприятием. Выявлены проблемы в сфере защиты информации отечественных предприятий. Исследованы различия в подходах к реализации мероприятий по обеспечению защиты информации промышленными предприятиями разного масштаба на рынке B2B. Выделены факторы, определяющие количественный и качественный состав способов и приемов защиты информации. Раскрыта суть и условия реализации принципа экономической целесообразности защиты информации. Проанализированы причины и последствия потерь предприятий в результате утечки информации. Определены различия в подходах к оценке потерь от утечки информации промышленными предприятиями разного масштаба на рынке B2B.

Ключевые слова: информация, защита информации, промышленные предприятия, экономическая целесообразность защиты информации, потери от утечки информации.

Deineha Oleksandr. INFORMATION SECURITY OF ENTERPRISES IN GLOBALIZATION CONDITIONS 4.0

The growth of informatization and computerization of production and management processes, the strengthening of international cooperation, increasing the openness of the information space of society, the unstable macroeconomic situation in Ukraine, the criminalization of society, the increase in unemployment, low level of solvency of the population, actualized the need for information protection at domestic enterprises operating in competitive environment. European companies have long recognized the feasibility of using information security policies in their own activities. Often, information security programs are implemented by enterprises that deal with information communications, professional scientific and technical activities, electric and gas steam generation and water conditioning, real estate operations. The problem of information security in most developed countries of the world is a priority and is considered at the state level. However, the majority of domestic enterprises still do not have a “culture of information protection”, that is, an understanding that their own information must be protected. The results of the research of the activity of industrial enterprises in the B2B market allowed to establish the main differences in the approaches to the implementation of measures to ensure the protection of information. To preserve information at enterprises, certain protective methods (organizational, technical, legal) may be used. In this case, the information security system should be adapted to the specific environment of the enterprise and its internal capabilities. That is why, for each individual enterprise, methods of protecting information can be different in scope and form. When ensuring the effective protection of information at enterprises, it is necessary to adhere to certain organizational and economic principles, the main of which are economic feasibility, activity, confidence, continuity, diversity, integrity (integrity) of information protection. The formation of a system of information security should primarily be carried out taking into account the principle of economic feasibility, that is, ensuring the optimal ratio of “protection of information / loss from information leakage”. Optimization is achieved by minimizing the cost of protecting information, but the lower

limit of costs can not be zero. Investigation of the relation of the management of industrial enterprises of the Rivne region to B2B sector to the estimation of losses from information leakage has made it possible to establish that only large enterprises partially estimate losses from information leakage (30,9%), with only a part of them (19,3%) used after that preventive measures to prevent information threats. With a decrease in the scale of enterprises, the level of scientific approach to the organization of information security is reduced.

Key words: information, information protection, industrial enterprises, economic feasibility of information protection, loss from information leakage.

Постановка проблеми. Інформація на протязі останніх десятиріч являється важливим активом підприємств. Ріст інформатизації та комп'ютеризації виробничих та управлінських процесів, посилення міжнародного співробітництва ще більше підвищили її цінність. Останнім часом реалії господарювання вітчизняних підприємств додатково ускладнилися нестабільною макроекономічною ситуацією в Україні, криміналізацією суспільства, підвищенням рівня безробіття, низьким рівнем платоспроможності населення тощо. За таких умов кожний господарюючий у конкурентному середовищі суб'єкт для підтримання своєї конкурентоздатності повинен забезпечувати захист важливої інформації, стосовно власної виробничої чи господарської діяльності. Посилює значення захисту інформації господарюючих суб'єктів і підвищення відкритості інформаційного простору життєдіяльності суспільства, пов'язаного із розвитком глобалізації, зокрема глобалізації 4.0.

Аналіз останніх досліджень і публікацій. Вирішенню проблем захисту інформації присвячена значна кількість наукових праць. У більшості з них експертами приділена значна увага технічним і організаційним питанням забезпечення захисту інформації [1; 2; 3; 4; 5; 6; 7], проте економічні аспекти формування систем захисту інформації у підприємницьких структурах або взагалі не розглядаються [4; 5], або це робиться дещо поверхово [1; 3; 6; 7].

Практичний досвід організовування систем захисту інформації на вітчизняних підприємствах досі визначається присутністю адміністративної економіки та ґрунтується на організації діяльності служб безпеки підприємств під контролем держави, проте методичне забезпечення зі створення систем захисту інформації на підприємствах всіх форм власності незалежно від масштабів їхньої діяльності (особливо малих) поки що є не досить розробленим. При цьому виникає низка проблем, найменш дослідженими з яких є економічні, зокрема пов'язані з тлумаченням самого об'єкта захисту та його характеристик, а також визначення оптимального співвідношення між витратами на захист інформації та можливими втратами від її витоку.

Формулювання цілей статті. Метою статті є дослідження організаційних і економічних проблем, що стосуються формування ефективної системи захисту інформації на підприємстві.

Виклад основного матеріалу дослідження. Підприємницькі структури та їх стейкхолдери у своїй діяльності все більше покладаються на використання інформаційних і комунікаційних технологій (ІКТ), а також сприяють швидкому прогресу у взаємодії організацій і споживачів продукції та послуг через Інтернет. У державному секторі ІКТ використовується для надання послуг, зберігання та обробки інформації, а також для забезпечення зв'язку з подальшою необхідністю захищати конфіденційність, безпеку та цілісність інформації, яка зберігається у державних системах управління.

Менеджмент підприємств ЄС здебільшого принципово визначився щодо доцільності застосування у власній господарській діяльності систем захисту власної інформації. Як свідчать дані, наведені на рис. 1, вони офіційно використовують політику інформаційної безпеки, причому великі підприємства більшою мірою визнають доцільність захисту власної інформації. Таке співвідношення може бути свідченням ще й того, що великі підприємства мають більше можливостей (фінансових, організаційних тощо) її реалізації.

Найчастіше програми інформаційної безпеки реалізують підприємства, які здійснюють інформаційні комунікації (60% усіх опитаних підприємств), професійну науково-технічну діяльність (49%), операції з нерухомістю (38%) та забезпечують електричну, газову парогенерацію та кондиціонування води (40 %) (рис. 2).

Дані, наведені на рис. 2, свідчать, що цінність інформації значно залежить від виду діяльності, яким займається підприємство, що, відповідно, визначає інтенсивність його зовнішніх комунікацій. Найбільшою цінність інформації є для підприємств, інформація для яких є і предметом, і засобом виробництва, і товаром (підприємства, що спеціалізуються на інформаційній діяльності та спілкуванні),

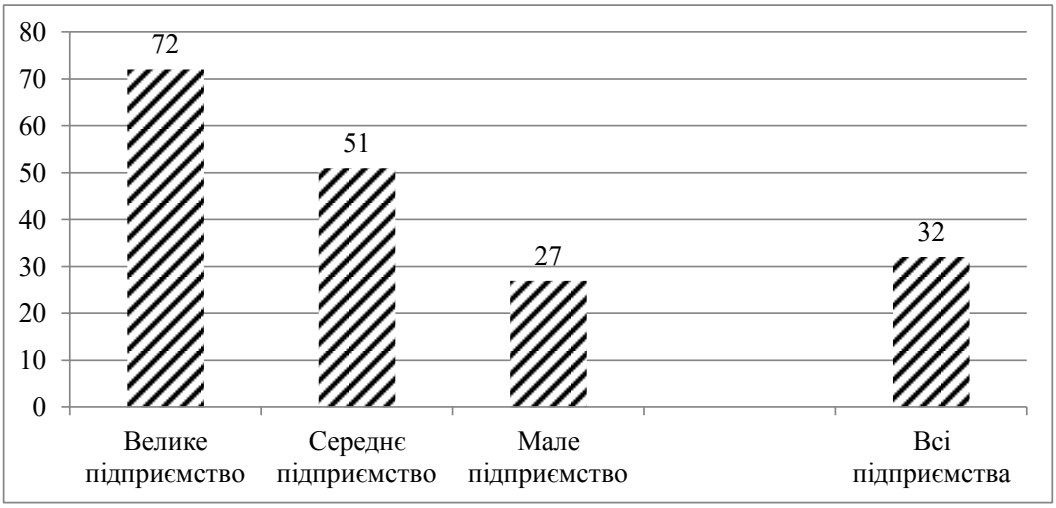

Рис. 1. Структурування за розміром підприємств, що офіційно застосовують політику інформаційної безпеки, 2015 рік (% підприємств) [8]

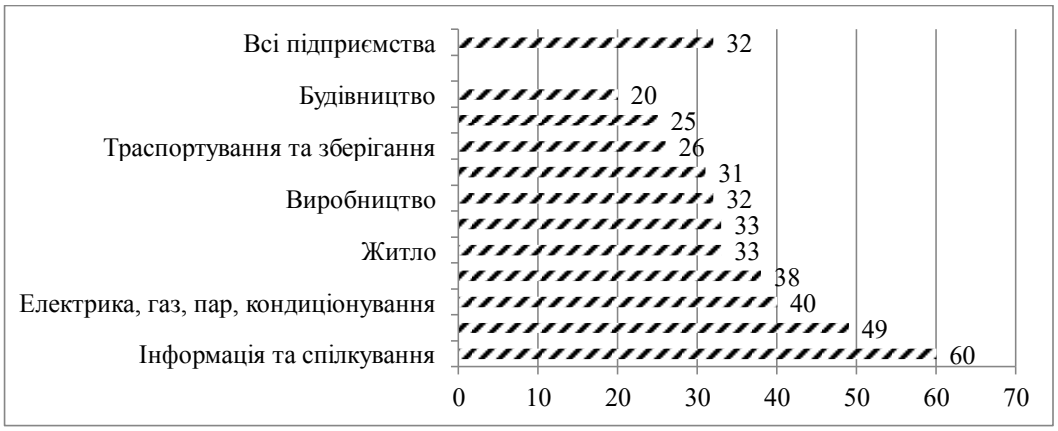

Рис. 2. Підприємства, що офіційно застосовують політику інформаційної безпеки, за видами економічної діяльності, 2015 рік (% підприємств) [8]

а найнижчою – для підприємств, що функціонують у сфері матеріального виробництва з найнижчим рівнем технологічних інновацій (наприклад, у будівництві).

Європейською практикою розглядаються такі інциденти, пов'язані з інформаційно-комунікаційними технологіями, що впливають на інформаційну систему підприємства та можуть спричинити проблеми конфліктів:

– знищення або пошкодження даних унаслідок апаратних або програмних збоїв, що спричиняє проблеми цілісності даних;

– недоступність інформаційних послуг через атаку ззовні, що спричиняється спробами ззовні зробити джерело інформаційної системи недоступним для своїх користувачів;

– розголошення конфіденційних даних через вторгнення, фармінг або фішингові атаки [9].

Проблема захисту інформації у більшості розвинутих держав світу є у пріоритеті та розглядається на державному рівні. Так, зокрема, уряд Австралії розробив основи політики забезпечення інформаційної безпеки та оприлюднив конкретні стратегії зменшення ризиків кібер-злочинів та напрями пов'язаного з ними контролю [10]. Однак, як показує українська практика, на більшості підприємств і досі не сформована «культура захисту інформації», тобто до виникнення критичної ситуації, що спричинена витоком важливої конфіденційної інформації, підприємець або відповідальний менеджер вважає, що діяльність його організаційної структури нікого не цікавить або що шпигунство – це явище несправжнє, суто літературне. Слід зазначити, що в умовах, коли на ринку при-

сутній більше, ніж один виробник (продавець) певного товару, між ними найчастіше виникає конкурентна боротьба, яка в умовах нерозвитого ринку нерідко є недобросовісною, а одним із методів недобросовісної конкуренції є, як відомо, промислове шпигунство, поява якого обумовлена розвитком ринкової системи господарювання, розпадом системи жорсткого контролю за виробництвом спеціальної техніки та ввезенням її в країну по офіційних і неофіційних каналах.

Неврегульованість чинного законодавства в сфері захисту інформації теж деякою мірою перешкоджає формуванню на вітчизняних підприємствах ефективних систем захисту інформації. Є більше тридцяти законів і нормативних документів у сфері захисту інформації, однак вони не завжди сприяють створенню передумов ефективного захисту інформації на підприємствах. Зокрема, йдеться про присутність різного роду доповнень, змін і уточнень до основних законодавчих актів, які найчастіше послаблюють правові можливості підприємств із погляду захисту інформації.

Крім того, на деяких підприємствах немає достатньої кількості вільних обігових коштів, які б могли бути спрямовані на забезпечення захисту інформації. Статистичні дані по Рівненській області свідчать про те, що більшість підприємств різного профілю не мають фінансових можливостей не лише для забезпечення формування повноцінних систем захисту інформації, а й для реалізації першочергових заходів із захисту інформації [11].

Результати дослідження промислових підприємств, які спеціалізуються на ринку B2B, дали змогу встановити такі основні відмінності у підходах до реалізації заходів із забезпечення захисту інформації. Менеджмент великих промислових підприємств сектору B2B найбільш пріоритетними з погляду забезпечення інформаційної безпеки бізнесу вважає ретельний відбір та звільнення працівників з урахуванням вимог із захисту інформації (41,8%) та підписання угод про нерозголошення комерційної таємниці (35,9%) (рис. 3-а). Варто зазначити, що такі підприємства застосовують комплексний підхід до побудови системи захисту інформації, мають власні служби безпеки. Середні за розміром промислові підприємства для збереження власних комерційних таємниць надають перевагу забезпеченню фізичної безпеки (37,1%), хоча і визнають необхідність реалізації таких організаційних заходів, як ретельний відбір та звільнення працівників (25,7%) (рис. 3-б). Малі промислові підприємства сектору B2B найбільше серед інших користуються послугами охоронних фірм (19,9%) і, на противагу великим і середнім, не мають досить фінансових ресурсів для створення власних служб безпеки, проте, беручи до уваги високу інтенсивність конкуренції на більшості товарних ринків, змушені приділяти увагу захисту інформації, що формує їхні конкурентні переваги на ринку. Саме тому малі і мікропідприємства серед усіх захисних заходів надають пріоритет забезпеченню фізичної безпеки, відповідно 48,3% та 65,4% (рис. 3-в, г).

Хоча захист інформації є важливим атрибутом існування підприємства, його організовування не зможе вирішити всі його проблеми. Необхідно пам'ятати про те, що найважливішим напрямом діяльності більшості підприємств є їх основна діяльність, спрямована на створення конкретного продукту, а захист інформації лише створює передумови для успішної діяльності підприємства в умовах конкурентного середовища. Саме тому основною метою системи захисту інформації є забезпечення умов для здійснення ефективної діяльності підприємства і всіх його підрозділів.

Для збереження інформації на підприємствах можуть бути використані певні захисні методи (організаційний, технічний, правовий), причому система захисту інформації повинна бути адаптована до специфіки зовнішнього середовища підприємства та його внутрішніх можливостей, а на кожному окремому підприємстві методи захисту інформації можуть бути різні за масштабами впровадження та формою.

Кількісний і якісний склад способів і прийомів захисту інформації залежить:

– від специфіки виробничої діяльності (найбільше потребують захисту інформації підприємства, котрі функціонують в умовах інтенсивної конкуренції, діяльність яких напряму залежить від якості інформації);

– від виробничих, фінансових й інших можливостей підприємства;

– від кількості таємних і конфіденційних відомостей, які використовуються конкретним підприємством і потребують захисту, а також корисності (цінності) інформації.

Під час забезпечення ефективного захисту інформації на підприємствах необхідно дотримуватися певних організаційно-економічних принципів, основними з яких є економічна доцільність, активність, впевненість, безперервність, різноманітність, комплексність (цілісність) захисту інформації тощо.

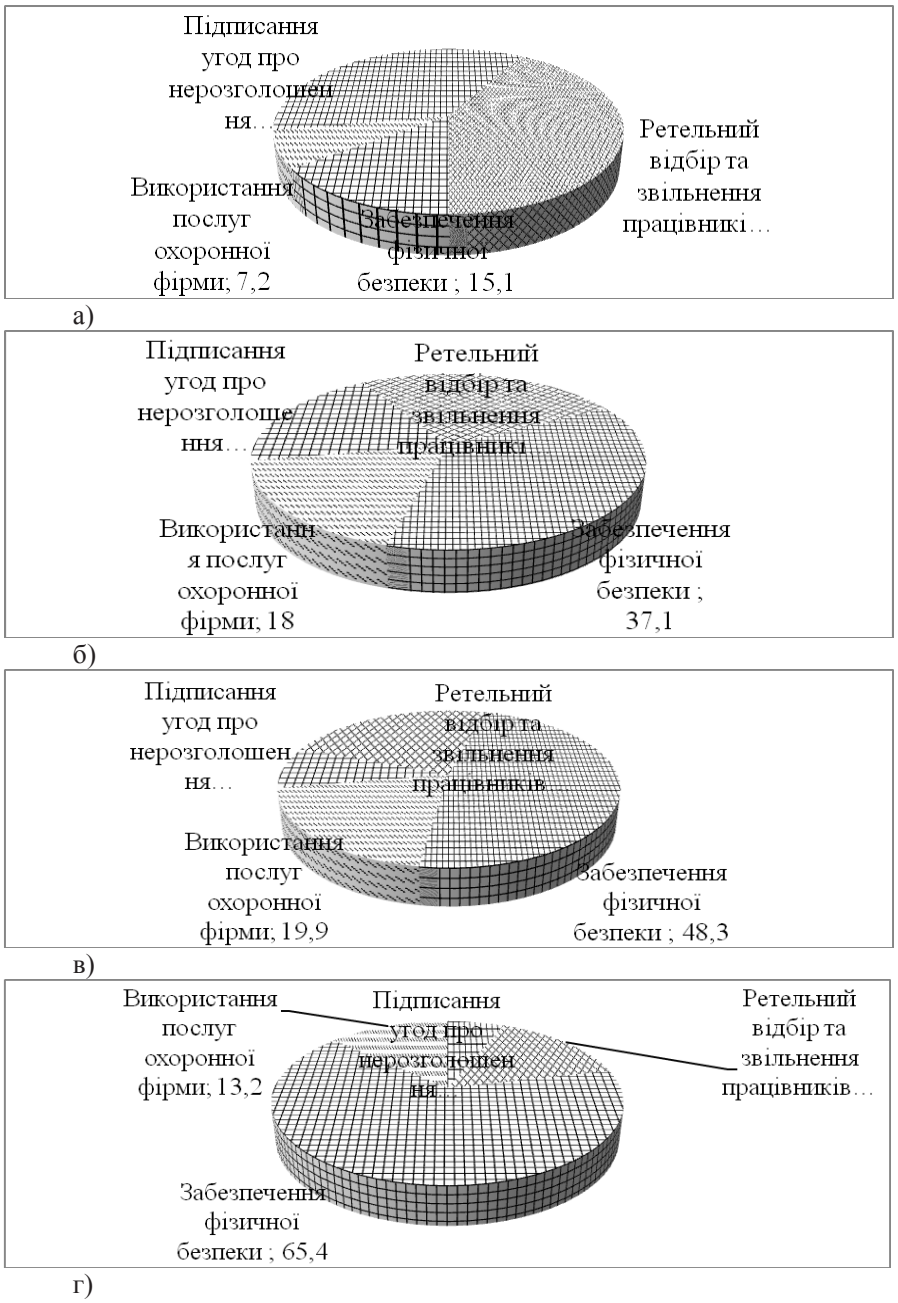

Рис. 3. Пріоритетність заходів із захисту інформації для промислових підприємств сектору B2B: а) великих; б) середніх; в) малих; г) мікро

Джерело: власне напрацювання

Формування системи захисту інформації повинно насамперед здійснюватися за принципом економічної доцільності, адже як халатне ставлення до зберігання (захисту) інформації, так і надмірне її засекречування однаковою мірою можуть викликати втрату частини прибутку чи призвести до непоправних економічних втрат. Формуючи перелік відомостей, які становлять комерційну таємницю, не слід також забувати і про те, що є й законодавчо зумовлена відповідальність за навмисне приховування інформації.

Як зазначає В. Бакланов, об'єктивно оцінити витрати на захист інформації дуже складно. Складність вирішення цього питання насамперед пояснюється тим, що реальні загрози для конкретного об'єкта не цілком визначені, а наслідки втілення цих загроз (завдані збитки) виявляються не завжди і не відразу [12, с. 78].

З погляду доцільності захисту всю інформацію підприємства можна поділити на відкриту (загальнодоступну), конфіденційну (з обмеженим доступом) та таємну (доступна тільки вузькому колу працівників підприємства, не доступна зовнішнім користувачам). Для того щоб забезпечити економічну доцільність захисту інформації, необхідно, щоб можливі втрати від витоку інформації були дещо більшими від витрат на її захист. Критичним рівнем витрат на захист інформації, вищим за який вони бути не можуть, буде величина ймовірних втрат від витоку інформації. Оптимізація досягається за мінімізації витрат на захист інформації, тобто чим нижчий рівень цих витрат, тим економічно доцільнішою є система захисту інформації. Однак нижня межа витрат, звісно, не повинна бути нульовою.

Економічна доцільність захисту інформації буде підвищуватися за рахунок скорочення витрат на захист інформації за одночасного підвищення (підтримки) загального рівня якості системи її захисту, тому встановлення можливих втрат від витоку певної інформації є завданням більше економічним, ніж організаційним. Адже від розрахованої величини можливих втрат від витоку інформації буде залежати величина коштів, що можуть будуть витрачені на її захист, а отже, і кількісний та якісний зміст складників системи захисту інформації на підприємстві.

Ця закономірність може бути використана також і для перевірки відповідності вже діючої системи захисту інформації на підприємстві вимозі економічної доцільності. При цьому вартісне значення витрат визначається на основі кошторису як сума видатків на проведення всіх захисних заходів.

Величина витрат на захист конкретної інформації повинна періодично переглядатися. Періодичність формування витрат на захист певної інформації буде залежати насамперед від інтенсивності її старіння, тобто проміжку часу, на протязі якого ця інформації може перейти з розряду особливо важливої до важливої та, врешті-решт, корисної або несуттєвої. Відповідно, найбільш важливим є завдання об'єктивної вартісної оцінки можливих втрат від витоку інформації. Спеціалісти всіх служб підприємства повинні навчитися правильно оцінювати (у вартісній формі) реальні та можливі втрати підприємства внаслідок витоку інформації.

Втрати від витоку інформації можуть бути спричинені такими обставинами, як втрата пріоритету в освоєних областях науково-технічного прогресу, зростання витрат на переорієнтацію діяльності дослідницьких підрозділів; втрата довіри споживача до якості продукції; виникнення чи створення конкурентами труднощів із закупівлею сировини, технологій, обладнання й інших компонентів, необхідних для здійснення нормальної виробничої діяльності; ускладнення відносин із партнерами, зрив вигідних контрактів і договірних зобов'язань; ріст витрат на створення нової ринкової стратегії, зміну плану проведення маркетингових досліджень тощо. Таким чином, ці втрати можуть бути прямими економічними (вартісними), тобто відразу вираженими в певній грошовій сумі; у вигляді втрати підприємством вигідного становища на ринку й ускладнень відносин із діловими партнерами, клієнтами.

У будь-якому разі втрати від витоку важливої конфіденційної інформації будуть економічними, лише тривалість їх трансформування може бути різною. Зокрема, ускладнення відносин із постачальниками може сприяти тому, що підприємство втратить доступ до дешевих сировинних ресурсів, що в свою чергу вплине на зростання прямих виробничих витрат і собівартості продукту. Зростання собівартості продукту приведе або до зростання ціни продукту (можливість втрати ринкової частки), або до зниження його рентабельності. І в тому, і в іншому разі підприємство втратить частину прибутку. Інший випадок – втрата довіри споживачів до якості продукту, яка може призвести до зниження обсягів та виручки від його реалізації та, відповідно, до втрати підприємством частини прибутку. Опосередковано втрати від витоку інформації можуть бути оцінені через корисність останньої.

Статистичні дані стосовно втрат від витоку інформації, що були оприлюднені закордонними організаціями, наведено в таблиці (табл. 1).

Дослідження ставлення менеджменту промислових підприємств Рівненщини сектору B2B до оцінювання втрат від витоку інформації дало змогу встановити, що лише переважно великі підприємства частково оцінюють втрати від витоку інформації (30,9%), причому тільки частина з них (19,3%) вжили після цього превентивних заходів із попередження інформаційних загроз. Менеджмент середніх підприємств ще менш розважливо підходить до оцінювання втрат від витоку інформації, адже 19,3% їх представників заявили про

Таблиця 1

Дані досліджень стосовно витоку інформації у 2014 році [13]

Обставина	Величина
Динаміка інформаційних злочинів	54% опитаних визначило, що втрати від витоку інформації зросли
Середня вартість витоку корпоративних даних	за останній рік збільшилася на 15% до 3,5 мільйонів доларів
Простій виробництва через порушення вимог інформаційної безпеки	зросли на 8 годин, характерно для 31% організацій
Середня вартість втраченої конфіденційної або таємної інформації	145,10 дол. США
Фінансові втрати фінансових організацій через втрату інформації	зросли на 24%
Середня вартість виплат за компрометуючий матеріал	найбільше заплатили компанії США і Німеччини, відповідно 246 і 215 дол.

можливість оцінювання таких втрат і лише 7,3% вжили превентивних заходів. На малих і мікропідприємствах теж приділяється недостатньо уваги оцінці втрат від витоку інформації (відповідно 27,4% і 27,7% здійснюють їх оцінювання). Проте одночасно спостерігається значна частка тих, хто взагалі або не може оцінити такі втрати, або не розуміє суті питання. Серед представників малих підприємств вона становила 72,6%, а мікро – 72,3%.

Намагаються застосовувати науково обґрунтований підхід до оцінювання втрат від витоку інформації переважно на великих підприємствах: 30,3% використовують при цьому статистичні методи, 20,6% – експертні і 23,7% – розрахунково-аналітичні. Лише 18,9% з них орієнтуються винятково на власну інтуїцію і лише 6,5% взагалі не оцінюють такі ризики з різних причин. Серед менеджменту середніх підприємств частка тих, хто не оцінює інформаційні ризики, становить вже майже третину (32,9%), а тих, хто використовує різні методи їх оцінювання, трохи менше половини (49%). Із зменшенням масштабів підприємств знижується рівень наукового підходу до організації захисту інформації. На малих підприємствах займаються оцінюванням ризиків втрати інформації лише 15,9 %, а на мікро – лише 7,9%, причому взагалі не вважають це важливим завданням та не оцінюють такі ризики відповідно 40,4% та 55,2%.

Ймовірність втрат від витоку інформації буде залежати від ймовірності виникнення загроз інформаційній безпеці підприємств. З огляду на природу загроз, що притаманні їх різним групам, можна виділити:

– навмисні загрози (ймовірність їх виникнення залежить від мотивації, знань, компетенції і ресурсів, що доступні потенційному злочинцю, а також від привабливості активів для реалізації атак);

– випадкові загрози (оцінюються з використанням статистики і досвіду, а їх ймовірність може залежати від близькості організації до джерел небезпеки (наприклад, автомагістралі, залізничні шляхи, заводи, що використовують у виробництві (виробляють) небезпечні речовини тощо);

– інциденти, що виникали в минулому (характеризують проблеми в захисних заходах, що використовуються підприємством);

– нові розробки і тенденції (включають у себе звіти, новини і тенденції, що отримані з Інтернету та інших джерел інформації) [14].

Для оцінювання ймовірності реалізації загрози А. Астахов пропонує застосовувати трирівневу якісну шкалу (табл. 2).

Втрата частини конфіденційної інформації про діяльність підприємства може призвести до серйозних економічних наслідків, підриває довіру ділових партнерів та споживачів підприємства до його діяльності, сприяє зниженню його ринкової вартості.

Точний вартісний розрахунок втрат від витоку інформації досить важкий, а часом і неможливий через відсутність якісних даних, а також через постійну динамічну зміну споживної вартості інформації, що потребує захисту. Тому інколи досить обмежитися зведеною експертною оцінкою. Експертами можуть виступати керівник підприємства, начальник служби безпеки, а також керівники відділів і служб підприємства, що мають доступ до важливої інформації. Вимога до підбору експертів одна – експерт повинен бути досить знайомий із проблемою і мати про неї власну думку, однак він не повинен бути зацікавлений в отриманні певного результату.

Таблиця 2

Масштабування загроз інформаційній безпеці підприємства

Рівень загрози	Ймовірність виникнення
низька	малоймовірно, що ця загроза буде реалізована, оскільки немає інцидентів, статистики, мотивів тощо, які би вказували на це. Очікувана частота реалізації не перевищує 1 разу на 5–10 років
середня	можливо, що ця загроза здійсниться (в минулому були інциденти, є відповідна статистика, є інформація, яка підтверджує, що вона можлива, тощо). Очікувана частота – приблизно 1 раз на рік
висока	ця загроза, швидше за все, здійсниться. Є інциденти, статистика або інша інформація, яка вказує на те, що загроза, швидше за все, здійсниться; є серйозні причини або мотиви для атакуючого, щоб здійснити такі дії. Очікувана частота – щонеділі або частіше

Джерело: узагальнення власне на підставі [14, с. 165-166]

Таблиця 3

Принципи захисту інформації

Принцип захисту інформації	Основний зміст
Активність	виражається в цілеспрямованому нав'язуванні технічній розвідці неправдивої інформації про об'єкт її розвідувальних наполягань у відповідності із задумом захисту
Впевненість	полягає у становленні захисту відповідно до обставин і залежно від характеру об'єкта, який захищають, або властивостей оточуючого середовища; у використанні рішень захисту, що відповідають кліматичним, сезонним та іншим умовам.
Безперервність	передбачає організацію захисту об'єкту на всіх стадіях його життєвого циклу «збір-обробка-знищення».
Різноманітність	передбачає виключення шаблонів, повторів у виборі об'єкту прикриття та шляхів реалізації змісту захисту, в тому числі з використанням типових рішень
Економічна доцільність	забезпечення оптимального співвідношення показників «витрати на захист інформації» / «ефект від використання інформації». Економічно доцільним є мінімізація витрат на захист інформації за одночасного зростання ефекту від її використання
Динамічність	комплекс заходів із захисту маркетингової інформації повинен періодично змінюватися (переглядатися). Це пов'язано насамперед із безперервним розвитком способів і засобів економічного шпигунства. Він повинен діяти рівно стільки часу, скільки необхідно для того, щоб розробити комплекс заходів із неправового збору цієї маркетингової інформації
Комплексність (цілісність)	на підприємстві повинні діяти всі захисні методи одночасно та з однаковою інтенсивністю, оскільки ефективність дії всієї системи буде визначатися якістю найгіршого її складника. Цілісність дії системи захисту маркетингової інформації виражається в наявності: єдиної мети її функціонування, інформаційних зв'язків між її елементами, ієрархічністю побудови підсистеми керування, системою захисту маркетингової інформації. Досягається за допомогою створення і координування ефективної роботи власної служби безпеки
Законності	побудова системи захисту маркетингової інформації повинна здійснюватися з дотриманням усіх наявних в країні законів і нормативних документів у сфері її захисту

Джерело: узагальнення власне на підставі [15, с. 252-258]

Крім принципу економічної доцільності, під час формування раціональних систем захисту інформації на підприємстві необхідно дотримуватися також і принципів активності, впевненості, безперервності, різноманітності, законності, динаміки, комплексності (табл. 3).

Для забезпечення захисту інформації підприємство може застосовувати організацій-

ний, технічний методи та здійснювати правове забезпечення захисту власної інформації.

На підприємстві повинні діяти всі захисні методи одночасно і з однаковою інтенсивністю. Це забезпечить виконання принципу комплексності (цілісності), оскільки ефективність дії всієї системи буде визначатися якістю найгіршого її складника. Цілісність дії системи захисту інформації буде також зумовлюватися: єдиною метою її функціонування, налагодженістю та узгодженістю інформаційних зв'язків між її елементами, ієрархічністю побудови підсистеми управління системою захисту інформації. Комплексність дії системи захисту інформації досягається за допомогою створення та координування ефективної роботи власної служби безпеки.

Висновки. Отже, система захисту інформації має лише відносно самостійне значення, оскільки в процесі свого функціонування вона обов'язково вступає у складні зв'язки з усіма іншими системами та підсистемами підприємства, його зовнішнім середовищем. Тому основною її метою є забезпечення нормального й ефективного функціонування системи вищого рівня управління, в яку вона вбудована і для якої створена, а саме системи управління підприємством.

Проблемі захисту інформації в сучасних умовах, які склалися, будь-яке підприємство повинно приділяти достатню увагу, оскільки це є одним із важливих аспектів, що забезпечує його ефективну роботу в умовах вільного конкурентного ринку.

Інформація, що формує конкурентні переваги підприємства, повинна бути захищена від можливої втрати (викрадення, випадкового знищення тощо). Проблема захисту інформації у більшості розвинутих держав світу є у пріоритеті та розглядається на державному рівні. Однак, як показує практика, на більшості вітчизняних підприємств і досі не сформована «культура захисту інформації». Крім того, на деяких підприємствах немає достатньої кількості вільних обігових коштів, які б могли бути спрямовані на забезпечення захисту інформації. Статистичні дані по Рівненській області свідчать про те, що більшість підприємств різної спеціалізації не мають фінансових можливостей не лише для забезпечення формування повноцінних систем захисту інформації, а й для реалізації першочергових заходів із захисту інформації. Створення надійної системи захисту інформації забезпечить збереження та розвиток конкурентних переваг підприємства на основі використання його інформаційних ресурсів.

ЛІТЕРАТУРА:

1. Духов В.Е. Экономическая разведка и безопасность бизнеса. Киев: ИМСО МО Украины, НВФ «Студцентр», 1997. 175 с.

2. Зубик В.Б., Седегов Р.С., Абдула А. Экономическая безопасность предприятия (фирмы). Минск: Выш. шк., 1998. 391 с.

3. Организация и современные методы защиты информации; под общ. ред. Диева С.А., Шаваева А.Г. Москва: Концерн «Банк.Дел.Центр», 1998. 472 с.

4. Чернявский А.А. Промышленный шпионаж и безопасность предпринимательства. Киев: МАУП, 1994. 64с.

5. Шиферский А.А. Защита информации: проблемы теории и практики. Москва: Юристь, 1996. 112с.

6. Ярочкин В. Коммерческая информация фирмы. Москва: Ось–89, 1997. 79 с.

7. Ярочкин В. Система безопасности фирмы. Москва: Ось-89, 1998. 192 с.

8. Enterprises having a formally defined ICT security policy, by size class, EU-28, 2015 (% enterprises). Eurostat Statistics. URL: http://ec.europa.eu/eurostat/statistics-explained/index.php/File:Enterprises_having_a_formally_defined_ICT_security_policy,_by_size_class,_EU-28,_2015_(%25_enterprises)_new.png (дата звернення: 01.02.2019)

9. ICT security in enterprises. *Eurostat Statistics.* URL: http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises (дата звернення: 01.02.2019)

10. Cyber Attacks: Securing Agencies' ICT Systems. *Australian National Audit Office*. URL: https://www.anao.gov.au/work/performance-audit/cyber-attacks-securing-agencies-ict-systems (дата звернення: 01.02.2019)

11. Головне управління статистики у Рівненській області. URL: http://www.rv.ukrstat.gov.ua/ (дата звернення: 01.02.2019)

12. Бакланов В.В. Введение в информационную безопасность. Направления информационной защиты. Екатеринбург: УрГУ, 2012. 235 с.

13. Shephard D. Fascinating & Scary IT Security Statistics. URL: https://www.netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/ (дата звернення: 01.02.2019)

14. Астахов А.М. Искусство управления информационными рисками. Москва: ДМКПресс, 2010. 312 с.
15. Крикавський Є.В., Дейнега О.В., Дейнега І.О., Шелюк Л.О., Кратт О.А., Патора Р. Маркетингова інформація. Львів: Видавництво Львівської політехніки, 2014. 416 с.

REFERENCES:

1. Dukhov V.Ye. (1997) Ekonomicheskaya razvedka i bezopasnost' biznesa [Economic intelligence and business security]. Kiyev: IMSO MO Ukrainy, NVF “Studtsentr”. (in Russian)
2. Zubik V.B., Sedegov R.S., Abdula A. (1998) Ekonomicheskaya bezopasnost' predpriyatiya (firmy) [Economic security of an enterprise (company)]. Minsk: Vysshaya shkola. (in Russian)
3. Organizatsiya i sovremennyye metody zashchity informatsii [Organization and modern methods of information protection]; pod obshch. red. Diyeva S.A., Shavayeva A.G. (1998) Moskva: Kontsern “Bank.Del.Tsentr”. (in Russian)
4. Chernyavskiy A.A. (1994) Promyshlennyy shpionazh i bezopasnost' predprinimatel'stva [Industrial espionage and enterprise security]. Kiyev: MAUP.
5. Shiferskiy A.A. (1996) Zashchita informatsii: problemy teorii i praktiki [Information security: problems of theory and practice]. Moskva: Yurist'. (in Russian)
6. Yarochkin V. (1997) Kommercheskaya informatsiya firmy [Commercial information of the company]. Moskva: Os'–89. (in Russian)
7. Yarochkin V. (1998) Sistema bezopasnosti firmy [Security system of the company]. Moskva: Os'-89. (in Russian)
8. Enterprises having a formally defined ICT security policy, by size class, EU-28, 2015 (% enterprises). Eurostat Statistics. Available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/File:Enterprises_having_a_formally_defined_ICT_security_policy,_by_size_class,_EU-28,_2015_(%25_enterprises)_new.png (accessed: 01.02.2019)
9. ICT security in enterprises. Eurostat Statistics. Available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises (accessed: 01.02.2019)
10. Cyber Attacks: Securing Agencies' ICT Systems. Australian National Audit Office. Available at: https://www.anao.gov.au/work/performance-audit/cyber-attacks-securing-agencies-ict-systems (accessed: 01.02.2019)
11. Holovne upravlinnya statystyky u Rivnens'kiy oblasti [The Main Department of Statistics in Rivne Oblast]. Available at: http://www.rv.ukrstat.gov.ua/ (accessed: 01.02.2019)
12. Baklanov V. V. (2012) Vvedeniye v informatsionnuyu bezopasnost'. Napravleniya informatsionnoy zashchity [Introduction to Information Security. Directions of information protection]. Yekaterinburg: UrGU. (in Russian)
13. Shephard D. Fascinating & Scary IT Security Statistics. Available at: https://www.netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/ (accessed: 01.02.2019)
14. Astakhov A.M. (2010) Iskusstvo upravleniya informatsionnymi riskami [The art of information risk management]. Moskva: DMKPress. (in Russian)
15. Krykavs'kyy YE.V., Deyneha O.V., Deyneha I.O., Shelyuk L.O., Kratt O.A., Patora R. (2014) Marketynhova informatsiya [Marketing Information]. L'viv: Vydavnytstvo L'vivs'koyi politekhniky. (in Ukrainian)