УДК: 338.4

Н.Г. Георгіаді
Національний університет "Львівська політехніка"

ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМИ УПРАВЛІННЯ ПІДПРИЄМСТВОМ

Уточнено сутності понять "інформаційна безпека" та "конфіденційна інформація"; виділено групи конфіденційної інформації на підприємстві; встановлено способи захисту конфіденційної інформації підприємства від її розголошення, витікання та несанкціонованого доступу до неї, визначено сутність системи захисту конфіденційної інформації підприємства та уточнено її складові.

The essences of concepts "informative safety" and "confidential information" are specified; the groups of confidential information on an enterprise are selected; the methods of defense of confidential information of enterprise are set from its disclosure, effluence and unauthorized division to her; the essence of the system of defense of confidential information of enterprise is certain and its constituents are specified in the article.

Постановка проблеми. Інформація, як і будь-який продукт, має виробників, споживачів і власників, а тому наділена певними споживчими якостями. З погляду споживача, якість використовуваної інформації дає змогу отримувати економічний або інші ефекти. З погляду власника, збереження в таємниці комерційно важливої інформації дає змогу успішно конкурувати на ринку виробництва і збуту товарів і послуг. Це відповідно вимагає певних дій, спрямованих на захист конфіденційної інформації. Задовольнити сучасні вимоги щодо безпеки підприємства і захисту його конфіденційної інформації можна формуванням системи інформаційної безпеки.

Аналіз останніх досліджень і публікацій. В економічній енциклопедії О. Горбатюк зазначає, що інформаційна безпека – це стан захищеності потреб особи, суспільства та держави в інформації незалежно від внутрішніх і зовнішніх загроз. Щодо можливих негативних впливів різних видів інформаційна безпека – це захищеність інформації та підтримуючої інфраструктури від випадкових чи навмисних природних або штучних впливів, які можуть заподіяти шкоду їхнім власникам або користувачам [1, с. 696].

У літературі з питань інформаційної безпеки виділяється поняття "конфіденційна інформація". На думку спеціалістів, відомості, які становлять конфіденційну інформацію і підлягають охороні, повинні відповідати таким категоріям [5, с. 622]:

- їх відкрите використання пов'язане зі збитками для підприємства;
- вони не є загальновідомими або загальнодоступними на законних підставах;
- підприємство може здійснити відповідні заходи зі збереження їх конфіденційності з огляду на економічну та іншу вигоди;
- ці відомості потребують захисту, оскільки вони не є держаними таємницями і не захищені авторським і патентним правом;
- приховування цих відомостей не наносить шкоди суспільству.

Вивчення літературних джерел [2, 3, 4, 5, 7] уможливлює укрупнено виділити три групи конфіденційної інформації підприємства:

1) науково-технічна інформація (характер науково-дослідних робіт; зміст патентів і ліцензій; зміст раціоналізаторських пропозицій; плани впровадження нових технологій і видів продукції; аналіз конкурентоспроможності продукції, що випускається підприємством);

2) виробнича інформація (технологія виробництва; обсяг випуску і плани реалізації продукції; рівень складських запасів; плани інвестицій у нове будівництво і реконструкцію

виробництва; методи і організація управління; система організації праці; плани рекламної діяльності; прогнозований час виходу на ринок; характер і умови укладених контрактів; відомості про постачальників, споживачів, посередників, конкурентів);

3) фінансова інформація (структура капіталів; розмір прибутку і рівень собівартості продукції; механізм формування цін на продукцію; відомості про банківські і торговельні операції; розмір обороту засобів; стан розрахунків з торговими клієнтами; рівень платоспроможності підприємства; фактичний стан ринків збуту; відомості про ефективність експорту і імпорту; відомості про фінансовий стан постачальників, споживачів, посередників, конкурентів тощо.)

До категорії конфіденційної не може належати інформація, яка міститься в: засновницьких документах; документах, що дають право займатись підприємницькою діяльністю (реєстраційні посвідчення, ліцензії, патенти); фінансовій звітності; документах про платоспроможність; документах про сплату податків та інших обов'язкових платежів до бюджету. Неконфіденційними також є відомості про: чисельність, склад працівників, їх заробітну плату, умови праці і наявність робочих місць; забруднення довкілля, порушення антимонопольного законодавства, недотримання безпечних умов праці, реалізація продукції, шкідливої для здоров'я населення, а також інші порушення законодавства і розміри завданої шкоди.

Як показує практика, у конкурентній боротьбі широко розповсюдженими є дії, спрямовані на отримання конфіденційної інформації різноманітними способами. Як зазначає В. Ярочкін, потенційні або реально можливі дії щодо інформаційних ресурсів, які призводять до неправомірного володіння відомостями, які охороняються, слід вважати загрозами конфіденційній інформації. Такими діями є: ознайомлення з конфіденційною інформацією різними шляхами і способами без порушення її цілісності; модифікація інформації в кримінальних цілях як часткова або значна зміна складу і змісту відомостей; руйнування (знищення) інформації як акт вандалізму з метою прямого нанесення матеріальних збитків. В кінцевому рахунку протиправні дії з інформацією призводять до порушення її конфіденційності, повноти, достовірності і доступності, що, своєю чергою, погіршує якість процесу управління в умовах неповної або хибної інформації [7, с. 18].

Як показує практика, щодо об'єкта управління загрози конфіденційній інформації можуть бути внутрішніми (які виникають всередині об'єкта) і зовнішніми (які виникають за межами об'єкта). Джерелами внутрішніх загроз є: адміністрація підприємства; персонал; технічні засоби забезпечення виробничої і трудової діяльності, а зовнішніх – недобросовісні конкуренти; злочинні угруповання і формування; окремі особи або організації адміністративно-управлінського апарату. У практиці підприємств близько 82 % загроз здійснюється власними працівниками підприємства за їх прямої або непрямої участі, 17 % загроз є зовнішніми, 1 % загроз здійснюється випадковими особами [7, с. 22].

Формулювання цілей статті. Цілями цієї роботи є: уточнення сутності понять "інформаційна безпека" та "конфіденційна інформація"; встановлення способів захисту конфіденційної інформації підприємства від її розголошення, витоку та несанкціонованого доступу до неї; уточнення складових системи захисту конфіденційної інформації підприємства.

Виклад основного матеріалу. За рівнем доступу до інформації доцільно виділяти конфіденційну, загальнодоступну та інформацію з обмеженим доступом. Конфіденційною слід вважати інформацію, доступ до якої можуть мати усі працівники підприємства за умови її нерозголошення. Інформація з обмеженим доступом – це частина конфіденційної інформації, до якої має доступ обмежене коло осіб. Загальнодоступною вважається інформація, умови використання якої не обумовлені.

Вивчення літературних джерел дає змогу виділяти такі дії, що призводять до незаконного володіння конфіденційною інформацією підприємства [5, 7]:

1) розголошення інформації;
2) витік інформації;
3) несанкціонований доступ до інформації.

Розголошення – це зловмисні або необережні дії з конфіденційними відомостями, що призводять до ознайомлення з ними осіб, не допущених до цих відомостей [7, с. 24]. Розголошення виражається у повідомленні, передачі, наданні, пересиланні, опублікуванні, втраті та інших формах обміну і дій з інформацією. Як правило, причинами розголошення конфіденційної інформації є: недостатнє знання працівниками підприємства правил захисту комерційних таємниць; нерозуміння їх ретельного дотримання; неусвідомлення потреби захисту інформації; відсутність на підприємстві системи контролю та покарання осіб за розголошення конфіденційної інформації. Суб'єктом у цьому процесі виступає джерело (власник) відомостей, що охороняються. За умови розголошення конфіденційної інформації необхідним є аналіз каналів розповсюдження, способів і засобів припинення розголошення.

Витік – це безконтрольний вихід конфіденційної інформації за межі організації або кола осіб, яким вона була довірена [7, с. 24]. При витоку конфіденційної інформації, як і при розголошенні, потрібно досліджувати канали витоку, способи і засоби захисту від нього. Під каналом витікання інформації прийнято розуміти фізичний шлях від джерела конфіденційної інформації до зловмисника, через який останній може отримати доступ до відомостей, що охороняються.

Несанкціонований доступ – це протиправне зумисне оволодіння конфіденційною інформацією особою, яка не має права доступу до неї [7, с. 25]. При несанкціонованому доступі до конфіденційної інформації слід звернути увагу на канали проникнення, способи і засоби протидії несанкціонованому доступу до інформації. У практичній діяльності іноземних спецслужб способами несанкціонованого доступу до джерел конфіденційної інформації можуть бути [5, с. 638]: підкуп, шантаж, переманювання працівників, заслання агентів; прослуховування телефонних розмов; викрадення документів; проникнення в комп'ютерну мережу.

Як показує практика, 90–95 % всієї необхідної інформації підприємство може отримати в легальний спосіб. Решта інформації отримується шляхом промислового шпіонажу. При цьому в 47 % випадків використовуються технічні засоби промислового шпіонажу. Повсякденна реальність вказує на тісне переплетіння в діяльності конкуруючих підприємств легальних і нелегальних методів одержання інформації один про одного.

Вивчення вітчизняних та зарубіжних літературних джерел дає змогу зробити висновок про те, що намітилась стійка тенденція до збільшення кількості зловмисних дій у сфері інформатизації. Для боротьби з цією тенденцією необхідним є організування цілеспрямованого процесу захисту інформації, до якого необхідно залучити професійних спеціалістів-розробників, працівників-користувачів на підприємстві тощо. При цьому цілями захисту інформації повинні бути:

- запобігання розголошенню, витоку і несанкціонованому доступу до відомостей, що охороняються;
- запобігання протиправним діям зі знищення, модифікації, спотворення, копіювання, блокування інформації;
- забезпечення правового режиму захисту документованої інформації як об'єкта власності;
- захист конституційних прав громадян на збереження особистої таємниці конфіденційності персональних даних, що містяться в інформаційних системах;
- збереження державної таємниці, конфіденційності документованої інформації відповідно до законодавства;
- забезпечення прав суб'єктів в інформаційних процесах і при розробці, впровадженні інформаційних систем, технологій і засобів їх забезпечення.

Як показує практика, забезпечення безпеки інформації не може бути одноразовим актом. Це безперервний процес реалізації найбільш раціональних методів, способів і шляхів удосконалення і розвитку системи захисту; контролю її стану, виявлення її слабких сторін і протиправних дій. Безпека інформації може бути забезпечена лише за комплексного використання усього арсеналу існуючих засобів захисту в усіх структурних підрозділах підприємства і на всіх етапах технологічного циклу обробки інформації. Найбільший ефект досягається тоді, коли усі засоби, методи і заходи об'єднуються в єдиний цілісний механізм – систему захисту інформації (СЗІ). При

цьому функціонування системи повинно контролюватись, оновлюватись і доповнюватись залежно від зміни внутрішніх і зовнішніх умов. Жодна СЗІ не може забезпечити необхідного рівня безпеки інформації без відповідної належної підготовки користувачів і дотримання ними усіх установлених правил, спрямованих на її захист.

Враховуючи сказане, під системою захисту інформації слід розуміти організовану сукупність спеціальних органів, засобів, методів і заходів, що забезпечує захист інформації від внутрішніх і зовнішніх загроз.

З позиції системного підходу до захисту інформації слід пред'являти певні вимоги. Захист інформації повинен бути: безперервним; плановим; цілеспрямованим; конкретним; активним; надійним; універсальним; комплексним. Безперервність полягає у постійному функціонуванні, удосконаленні і розвитку СЗІ. Планування здійснюється шляхом розробки кожним структурним підрозділом ретельних планів захисту інформації у межах його компетенції із врахуванням загальної мети підприємства. Цілеспрямованість передбачає захист того, що повинно захищатись в інтересах конкретної цілі. Конкретність полягає у захисті конкретних даних, втрата яких може спричинити підприємству певний збиток. Активність має на меті захист інформації з достатнім рівнем наполегливості. Методи та форми захисту повинні надійно перекривати можливі шляхи неправомірного доступу до інформації. Універсальність полягає у тому, що незалежно від виду, характеру і форми інформації вона повинна бути захищена наявними засобами і можливими методами і заходами. Комплексність передбачає захист інформації кожного структурного підрозділу і підприємства в цілому комплексом наявних засобів та можливих методів і заходів.

До СЗІ слід пред'являти також певні вимоги: чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації; надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи; зведення до мінімуму числа спільних для декількох користувачів засобів захисту; облік випадків і спроб несанкціонованого доступу до конфіденційної інформації; забезпечення оцінки ступеня конфіденційності інформації; забезпечення контролю цінності засобів захисту і негайне реагування на їх вихід з ладу.

Зарубіжний і вітчизняний досвід показує, що для забезпечення виконання цих вимог безпеки, СЗІ повинна діяти відповідно до певних умов [7, с. 10]: охоплювати весь технологічний комплекс інформаційної діяльності; бути різноманітною за використовуваними засобами, багаторівневою з ієрархічною послідовністю доступу; бути відкритою для змін і доповнень заходів забезпечення безпеки інформації; бути нестандартною, різноманітною; бути простою для технічного обслуговування і зручною для експлуатації користувачами; бути надійною, оскільки будь-які поламки технічних засобів є причиною появи неконтрольованих каналів витоку інформації; бути комплексною, володіти цілісністю, що означає, що жодна її частина не може бути вилучена без втрати для всієї системи.

Вивчення літературних джерел і практики діяльності вітчизняних та зарубіжних підприємств дає змогу виділяти такі напрямки захисту інформації [7, с. 31]:

1) правовий захист, який ґрунтується на спеціальних законах, нормативних актах, правилах, процедурах і заходах, що забезпечують захист інформації на правовій основі;

2) організаційний захист, тобто регламентація виробничої діяльності і взаємовідносин між виконавцями на нормативно-правовій основі, яка виключає або послаблює неправомірне оволодіння конфіденційною інформацією і прояв внутрішніх і зовнішніх загроз;

3) інженерно-технічний захист, тобто використання технічних засобів і заходів з їх використання в інтересах захисту конфіденційної інформації.

Відповідно до встановлених напрямків можна виділити такі групи заходів із захисту конфіденційної інформації:

1) організаційні, тобто заходи обмежувального характеру, які зводяться до регламентації доступу і використання технічних засобів обробки інформації. Вони, своєю чергою, включають:

- територіальні обмеження (уміле розташування радіоелектронних засобів на місцевості, що унеможливлює перехоплення радіосигналів);
- просторові обмеження (вибір напрямків випромінювання в бік найменшої можливості перехоплення);
- часові обмеження (скорочення до мінімуму тривалості випромінювання);

2) організаційно-технічні заходи, які забезпечують блокування можливих каналів витоку інформації через технічні засоби за допомогою спеціальних пристроїв, що встановлюються на елементи конструкцій будівель, приміщень і технічних засобів обробки інформації. Вони, своєю чергою, бувають:

- просторові (зменшення ширини діаграми направленості, послаблення бокових і задньої пелюсток діаграми направленості);
- режимні (використання прихованих методів передачі інформації);
- енергетичні (зниження інтенсивності випромінювання і робота на знижених потужностях);

3) технічні заходи, тобто придбання, встановлення і використання захищених від побічних електромагнітних випромінювань і наведення, а також акустичних впливів технічних засобів обробки інформації. Технічні заходи передбачають:

- приховування (використання радіомовчання, створення пасивних перешкод);
- придушення (створення активних перешкод);
- дезінформація (організація удаваної роботи, зміна режимів використання частот і регламентів зв'язку, показ хибних демаскуючих ознак).

Вивчення літературних джерел дає змогу відповідно до встановлених напрямків і заходів виділити способи захисту конфіденційної інформації від її розголошення, витікання та несанкціонованого доступу до неї (таблиця).

Способи захисту конфіденційної інформації від її розголошення, витоку та несанкціонованого доступу до неї

Дії, що призводять до незаконного володіння конфіденційною інформацією	Фактори спричинення дій, що призводять до незаконного володіння конфіденційною інформацією підприємства	Умови спричинення дій, що призводять до незаконного володіння конфіденційною інформацією підприємства	Способи захисту інформації від дій, що призводять до незаконного володіння конфіденційною інформацією підприємства
1	2	3	4
Розголошення конфіденційної інформації	• недостатні знання працівників правил захисту конфіденційної інформації і нерозуміння необхідності ретельного їх виконання • слабкий контроль за дотриманням правил роботи з відомостями конфіденційного характеру • плинність кадрів, у тому числі тих, що володіють відомостями конфіденційного характеру тощо	• передавання інформації каналами електрозв'язку • здійснення повідомлень, оголошень на зустрічах, переговорах, виставках тощо • пересилання документів • опублікування документів • втрата документів • безконтрольна розробка документів • безконтрольне зберігання і знищення документів тощо	• складання переліку відомостей, що становлять конфіденційну інформацію підприємства • доведення цього переліку до кожного працівника підприємства • внесення до обов'язків кожного працівника підприємства необхідність збереження конфіденційної інформації в таємниці • запровадження системи контролю за збереженням конфіденційної інформації

Продовження таблиці

1	2	3	4
Витік конфіденційної інформації	• недостатні знання працівників правил захисту конфіденційної інформації і нерозуміння необхідності ретельного їх виконання • слабкий контроль за дотриманням правил захисту інформації правовими, організаційними та інженерно-технічними заходами • плинність кадрів, у тому числі тих, що володіють відомостями конфіденційного характеру тощо	Витік інформації такими каналами: • візуально-оптичними • акустичними • електромагнітними • матеріально-речовими Причинами виникнення каналів витоку інформації можуть бути: • недосконалість схемних рішень (конструктивні, технологічні) • експлуатаційний знос елементів (зміна параметрів, аварійний вихід з ладу) тощо	• виявлення, облік і контроль можливих каналів витоку конфіденційної інформації в конкретних умовах захисту об'єкта • здійснення організаційних, організаційно-технічних та технічних заходів із захисту інформації від витоку технічними каналами • запровадження системи контролю за станом заходів із захисту конфіденційної інформації
Несанкціонований доступ до конфіденційної інформації	• недостатні знання працівників правил захисту конфіденційної інформації і нерозуміння необхідності ретельного їх виконання • слабкий контроль за дотриманням правил захисту інформації від несанкціонованого доступу до неї використання недосконалих технічних засобів зберігання і обробки конфіденційної інформації тощо	• ініціативна співпраця • схиляння до співпраці • вивідування, випитування • підслуховування • спостереження • викрадення • копіювання • підробка (модифікація) • знищення • незаконне підключення • перехоплення • негласне ознайомлення • фотографування • збирання і аналітична обробка інформації тощо	• виявлення, облік і контроль можливих способів несанкціонованого доступу і проникнення до джерел конфіденційної інформації • здійснення організаційних, організаційно-технічних та технічних заходів із протидії несанкціонованому доступу запровадження системи контролю допуску і доступу до конфіденційної інформації підприємства на усіх рівнях управління

Висновки та перспективи подальших досліджень. Узагальнюючи вищесказане, можна виділити такі складові системи захисту конфіденційної інформації підприємства:

- регламентований перелік відомостей, що становлять конфіденційну інформацію підприємства;
- система обліку і охорони нових матеріалів і продукції;
- система охорони території підприємства, його будівель і споруд;
- система контролю за відвідуванням підприємства сторонніми особами;
- порядок діловодства з документами, що містять конфіденційну інформацію;
- система контролю за засобами копіювання і розмноження документів;
- порядок захисту інформації в засобах зв'язку і обчислювальної техніки;
- порядок використання відкритих каналів зв'язку під час передачі конфіденційної інформації;
- система мотивування і навчання персоналу підприємства способам захисту конфіденційної інформації;
- спеціалізовані служби з питань захисту конфіденційної інформації підприємства.

Проведені дослідження показали, що інформаційна безпека – це принцип побудови інформаційних систем управління підприємствами, зокрема, інтегрованих. Він реалізовується шляхом визначення конфіденційної управлінської інформації, передбачення можливих джерел розголошення, витікання і несанкціонованого доступу до інформації, формування системи заходів із захисту інформації. Одночасно інформаційна безпека є однією з якісних характеристик інформаційних систем управління підприємством. Вона відображає фактичний та потенційний рівень захищеності конфіденційної управлінської інформації від розголошення, витікання та несанкціонованого доступу.

Узагальнення літературних джерел і ознайомлення з матеріалами діючих підприємств дають змогу стверджувати, що реалізація принципу інформаційної безпеки під час побудови інформаційної системи управління підприємством значною мірою зазнає впливу таких чинників, як: фінансові і технологічні можливості підприємства; його розмір і розміщення; номенклатура продукції, що випускається; система внутрішнього документообігу; зміст, обсяг та види конфіденційної інформації, рівень інформаційної освіти працівників підприємства тощо. Перспективами подальших розвідок є визначення змісту цих чинників та рівня їх впливу на реалізацію вказаного та інших принципів формування інформаційної системи управління підприємством.

1. Економічна енциклопедія. У 3-х т. Т.1 / Редкол. … С.В. Мочерний (відп. ред.) та ін. – К., 2000. 2. Information Superhijhway: An Overview of tehnology Chnology Challenjes, Report to the USA Congres, 1995. 3. Матвієнко О.В., Цивін М.Н. Основи менеджменту інформаційних систем: Навч. посібник. – К., 2005. 4. Roche E.M. Managing Information Technology in Multinational Corporations. – New York: Macmillan Publishing kompany, 1992. 5. Справочник директора предприятия / Под ред. проф. М.Г. Лапусты. – М., 2003. 6. Что значит быть лидером? // COMPUTERWORLD/УКРАИНА. Информ.-аналитич. еженедельник. – 2005. – № 3–4 (485). – С. 27. 7. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М., 2003.

УДК 338.4

М.Ф. Гончар, О.Є. Кузьмін
Національний університет "Львівська політехніка"

ОЦІНЮВАННЯ ЯКОСТІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ

Здійснено спробу побудувати системи показників якості інформаційного забезпечення процесу прийняття управлінських рішень. Ця система містить показники точності, повноти, значущості, ефективності та оперативності інформаційного забезпечення управлінської діяльності. Проаналізовано вплив якості інформаційного забезпечення на якість управлінських рішень, що приймаються.

The attempt of construction of the system of indexes of qualities of the informative providing of process of decision-making administrative is carried out in the article. This system contains the indexes of exactness, plenitude, meaningfulness, efficiency and operativeness of the informative providing of administrative activity. Influence of qualities of the informative providing is analysed on qualities of administrative decisions which are adopted.

Постановка проблеми. Інформація являє собою основу процесу управління. Без її наявності неможливо сформувати цілі управління, оцінити ситуацію, визначити проблему, підготувати і прийняти управлінське рішення, проконтролювати його виконання.