УДК 510.004

Д.Б. Мехед, канд. пед. наук
Чернігівський національний технологічний університет, м. Чернігів, Україна

ЗАХИСТ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Д.Б. Мехед, канд. пед. наук
Черниговский национальный технологический университет, г. Чернигов, Украина

ЗАЩИТА ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Dmytro Mekhed, PhD in Pedagogical Sciences
Chernihiv National Technological University, Chernihiv, Ukraine

DATA PROTECTION ON THE ENTERPRISE

Розглянуто основні етапи захисту інформації на підприємстві. Визначено основну форму ведення аналітичної роботи. Висвітлено важливість проведення такої роботи на підприємстві в умовах сьогодення.

***Ключові слова**: захист інформації, аналітична робота, аналітичні звіти.*

Рассмотрены основные этапы защиты информации на предприятии. Определена основная форма ведения аналитической работы. Освещены важность проведения данной работы на предприятии в условиях современности.

***Ключевые слова:** защита информации, аналитическая работа, аналитические отчёты.*

The article describes the main stages of information security in the enterprise. Identify the main types of conducting analytical work. Highlighted the importance of this work in the enterprise in terms of modernity.

***Key words:** information security, analytical work, analytical account.*

Постановка проблеми. Нині в Україні у зв'язку з входженням у світовий інформаційний простір швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Створюються локальні і регіональні обчислювальні мережі, великі території охоплені мережами стільникового зв'язку, факсимільний зв'язок став доступний для широкого кола користувачів. Системи телекомунікацій активно впроваджуються у фінансові, промислові, торгові і соціальні сфери. У зв'язку з цим різко зріс інтерес широкого кола користувачів до проблем захисту інформації [3]. Аналіз стану захисту інформації – це комплексне вивчення фактів, подій, процесів, явищ, пов'язаних з проблемами захисту інформації, у тому числі даних про стан роботи по виявленню можливих каналів витоку інформації, про причини й обставини, що сприяють витоку і порушень режиму секретності (конфіденційності) у ході повсякденної діяльності підприємства. Аналітична робота – один з основних видів діяльності для забезпечення інформаційної безпеки будь-якого підприємства.

Аналіз останніх досліджень і публікацій. Дослідженню інформаційної безпеки присвячені роботи В.В. Баранника, В.М. Богуна, С.В. Віхорева, І.Д. Горбенко, Ю.І. Грицюк, С.В. Казмирчук, Г.Ф. Конаховича, О.Г. Корченка, М.Г. Луцького, А.І. Марущака, В.П. Мельнікова, В.В. Мохора, О.М. Новікова, О.В. Олійника, О.В. Сосніна, С.В. Толюпи, В.О. Хорошко, О.К. Юдіна та ін.

Дослідження різноманітних аспектів інформаційно-аналітичної діяльності здійснювали Т.В. Абрамова, С.С. Алдишев, В.П. Александрова, А.А. Атаян, С.Ф. Багаундінова, Т.В. Вдовіна, А.В. Горячов, Р.О. Гуревич, М.І. Жалдак, О.П. Значенко, В.Г. Кальченко, Н.В. Кисіль, В.І. Клочко, Н.В. Морзе, С.Ю. Нікіфорова, О.В. Пархоменко, С.А. Раков, М.В. Селіна, Ю.М. Ткач, В.А. Сластьонін та ін.

Виділення не вирішених раніше частин загальної проблеми. Проте, незважаючи на значний обсяг накопичених у цій сфері знань, недостатньо дослідженою залишилась проблема організації захисту інформації на підприємстві.

Мета статті. Головною метою цієї роботи є визначення основних етапів організації роботи у сфері захисту інформації на підприємстві.

Виклад основного матеріалу. Захист інформації на підприємстві – це вироблення ефективних заходів, пропозицій і рекомендацій керівництву підприємства, спрямованих на недопущення витоку конфіденційної інформації про діяльність підприємства і проведені роботи [1]. Основною ефективного захисту інформації є аналітична робота,

яка повинна включати елементи прогнозування можливих загроз. Основні напрямки аналітичної роботи на підприємстві такі: аналіз об'єкта захисту; аналіз внутрішніх і зовнішніх загроз інформаційної безпеки підприємства; аналіз можливих каналів несанкціонованого доступу до інформації; аналіз системи комплексної безпеки об'єктів; аналіз порушень режиму конфіденційності інформації; аналіз передумов до розголошення інформації, а також до втрати носіїв конфіденційної інформації. Функції аналізу на підприємстві покладаються на спеціально створений у його структурі аналітичний підрозділ, який комплектується кваліфікованими фахівцями в галузі захисту інформації [1]. Разом з тим такі фахівці повинні повною мірою володіти інформацією за всіма напрямками діяльності підприємства: знати види, характер і послідовність виконання виробничих робіт, взаємодіючі організації, специфіку діяльності структурних підрозділів підприємства і т. ін. Переважно аналітичний підрозділ включається до складу служби безпеки підприємства.

Аналітичний підрозділ повинен забезпечувати керівництво підприємства достовірною та аналітично обробленою інформацією, необхідною для прийняття ефективних управлінських рішень в усіх напрямках захисту інформації. Основними функціями аналітичного підрозділу є: забезпечення своєчасного надходження достовірних і всебічних відомостей з проблем захисту інформації; облік, узагальнення та постійний аналіз матеріалів про стан справ у системі захисту інформації підприємства (його філій та представництв); аналіз можливих загроз захисту інформації, моделювання реального сценарію можливих дій конкурентів (зловмисників), які зачіпають інтереси підприємства; забезпечення ефективності роботи з аналізу наявної інформації, виключення дублювання при її зборі, обробленні та розповсюдженні; моніторинг ситуації на ринку продукції, товарів і послуг, а також у зовнішньому середовищі з метою виявлення подій і фактів, які можуть мати значення для діяльності підприємства; забезпечення безпеки власних інформаційних ресурсів, обмеження доступу співробітників підприємства до аналітичної інформації; підготовка висновків і пропозицій, спрямованих на підвищення ефективності планованих і здійснюваних заходів щодо захисту інформації, а також уточнення (коригування) організаційно-плануючих документів підприємства та його структурних підрозділів; вироблення рекомендацій щодо внесення змін і доповнень у методичні документи, які регламентують алгоритм дій співробітників підприємства щодо захисту інформації (стандарти підприємства) [4].

Наявність постійної аналітичної роботи, її характер і результати визначають необхідність, основи організації, структуру та зміст системи комплексного захисту інформації, вимоги до її ефективності та напрямки її розвитку і вдосконалення [5]. Аналіз стану системи захисту інформації суттєво впливає на кількість, склад і структуру підрозділів підприємства, які безпосередньо вирішують ці завдання (служба безпеки підприємства, служба охорони, режимно-секретний підрозділ та ін.). Від ефективності та якості ведення на підприємстві аналітичної роботи повною мірою залежить стан захищеності інформаційних ресурсів підприємства, віднесених до категорії охоронюваних, а також своєчасність і обґрунтованість прийняття заходів щодо недопущення витоку конфіденційної інформації та втрат носіїв інформації. Ефективність аналітичної роботи та її результати є основою для прийняття керівництвом підприємства управлінських рішень з питань організації захисту інформації. З урахуванням результатів аналітичної роботи можуть проводяться такі основні заходи: уточнення (доробка) планів роботи підприємства щодо захисту інформації, включення до них додаткових заходів; уточнення розподілу завдань і функцій між структурними підрозділами підприємства; перероблення (уточнення) посадових (функціональних) обов'язків співробітників підприємства, у тому числі керівної ланки, вдосконалення систем пропускного і внутрішньооб'єктового режимів; обмеження кола осіб, які допускаються до конфіденційної

інформації з різних напрямків діяльності підприємства; перегляд ступеня конфіденційності відомостей та їх носіїв; посилення системи охорони підприємства та його об'єктів, застосування особливих заходів захисту інформації на окремих об'єктах (у службових приміщеннях); прийняття рішень про обмеження публікації у відкритій пресі, використання в рекламній та видавничій діяльності окремих матеріалів (матеріалів з окремих тем), доступу відряджених осіб, про виключення розгляду цих матеріалів на конференціях, семінарах, зустрічах тощо.

Ведення ефективної аналітичної роботи можливе лише за наявності необхідної інформації. Для її отримання потрібна чітко сформульована мета, що визначає конкретні джерела інформації. Аналітична робота на підприємстві повинна вестися послідовно і безперервно, являти собою повною мірою цілісне дослідження. В аналітичній роботі можна виділити такі основні етапи: формулювання цілей аналітичної роботи, розроблення програми досліджень, формулювання попередніх гіпотез (результатів аналітичної роботи); відбір і аналіз джерел інформації, збір та узагальнення інформації; повноцінний аналіз наявної інформації та підготовка висновків.

Основна форма ведення аналітичної роботи – аналітичні дослідження. Проведення аналітичних досліджень вимагає чіткої організації процесу, оцінювання наявних ресурсів для виконання досліджень і досягнення необхідного результату. Підсумком дослідження повинні бути висновки, пропозиції та рекомендації щодо вдосконалення системи захисту інформації. На першому етапі аналітичного дослідження формулюються цілі та завдання дослідження, розробляється програма дослідження, яка становить наукову основу збору, узагальнення, обробки та аналізу всієї отриманої інформації. Типова програма досліджень включає такі основні розділи: цілі і завдання аналітичного дослідження; предмети й об'єкти дослідження; терміни (період) проведення аналітичного дослідження; методики проведення дослідження; очікувані результати і передбачувані висновки. При формулюванні цілей і завдань дослідження потрібно враховувати, хто є його організатором і безпосереднім виконавцем, які сили і засоби можуть бути задіяні для його проведення, які будуть використовуватися джерела інформації, способи і методи її збору, обробки та аналізу, які існують можливості для реалізації пропозицій і рекомендацій, які будуть вироблені у ході досліджень.

Залежно від поставлених цілей і завдань визначаються конкретні методи і технології дослідження, а також процедури збору й обробки інформації. Найбільш типові такі завдання аналітичного дослідження: отримання даних про стан системи захисту інформації на підприємстві (його конкретних об'єктах, у філіях, представництвах); виявлення можливих каналів витоку інформації, що підлягає захисту; визначення обставин, причин і факторів, що сприяють виникненню каналів витоку і створенню передумов для витоку інформації; підготовка для керівництва підприємства (філії, представництва) та його структурних підрозділів конкретних рекомендацій щодо закриття виявлених каналів витоку. Під об'єктом дослідження розуміється все те, що вивчається та аналізується у ході дослідження. Предмет дослідження – та сторона об'єкта, яка безпосередньо підлягає вивченню у ході аналітичного дослідження. Особливе значення на першому етапі аналітичної роботи має формулювання попередніх гіпотез (версій). Попередні гіпотези повинні пояснити роль і місце висновків аналітичних досліджень у логічній послідовності подій, що відбуваються у сфері захисту охоронюваної інформації.

Побудова попередніх гіпотез проводиться в такому порядку. Спочатку формується повний список відомостей, які передбачається дослідити (проаналізувати). Відомості, що увійшли у список, систематизуються і розташовуються за ступенем важливості. Далі з усього обсягу інформації виділяється група найбільш значущих відомостей, роль яких особливо очевидна в ситуації, що підлягає аналізу та оцінюванню. Обрані відомості класифікуються за актуальністю, способом отримання та ступенем достовірності

джерела. Найбільш актуальні відомості аналізуються в першу чергу. Потім проводиться вибір попередніх гіпотез, що пояснюють прояви тих чи інших подій (поява тих чи інших відомостей). Причому відносно однієї події здійснюється перевірка декількох гіпотез (версій). При послідовній перевірці гіпотез особлива увага приділяється найбільш реальним. Ці гіпотези фіксуються. Найменш реальні гіпотези відхиляються. Таким чином, послідовно вибираються і формулюються найбільш імовірні припущення, що пояснюють появу тих чи інших конкретних подій (виникнення відомостей). Можливі суперечності в отриманих висновках про передбачувані версії подій, що відбуваються, усуваються через всебічну послідовну перевірку реальності гіпотез.

Результатом роботи по формулюванню попередніх гіпотез є вибір версії, яка найбільш точно порівняно з іншими версіями пояснює причину виникнення конкретної ситуації, пов'язаної з появою можливого каналу витоку конфіденційної інформації, і характеризує стан системи захисту інформації, у тому числі дії відповідних посадових осіб, якість виконання заходів і т. ін. На другому етапі проводиться відбір і аналіз джерел інформації, збір та узагальнення даних з метою виявлення каналу несанкціонованого доступу до відомостей конфіденційного характеру, виключення можливості виникнення такого каналу. Для цього здійснюється постійний контроль об'єктів захисту (інформаційних ресурсів), а також ступеня захищеності оброблюваної (циркулюючої) в них інформації, проводиться аналіз даних, одержуваних з різних джерел. Для вирішення конкретного завдання аналітичного дослідження в межах другого етапу з усіх наявних у розпорядженні аналітичного підрозділу джерел інформації відбираються ті, з яких надходить інформація, найбільш близька до досліджуваних проблем, і водночас достатньо достовірна.

Аналітичне дослідження джерел інформації передбачає проведення таких основних заходів: формування вичерпного переліку джерел конфіденційної інформації на підприємстві; формування і своєчасне уточнення переліку та складу конфіденційної інформації, реально циркулюючої (оброблюваної) на об'єктах підприємства, з зазначенням конкретних носіїв, на яких вона зберігається; організація та ведення обліку обізнаності співробітників підприємства в конфіденційної інформації, накопичення даних про їх ознайомлення з конкретними відомостями конфіденційного характеру з зазначенням носіїв цих відомостей; вивчення та оцінка відповідності ступеня конфіденційності, присвоєної інформації, реальної цінності цієї інформації; вивчення внутрішніх і зовнішніх загроз кожному наявному на підприємстві джерелу конфіденційної інформації; виявлення підприємств, зацікавлених в отриманні конфіденційної інформації (фірм-конкурентів), а також окремих осіб-зловмисників та їх систематизація (класифікація); аналіз повноти та якості заходів щодо захисту конфіденційної інформації, що приймаються (прийнятих) у конкретних ситуаціях. Облік і аналіз спроб представників фірм-конкурентів, а також інших зловмисників отримати конфіденційну інформацію; облік і аналіз контактів співробітників підприємства з представниками фірм-конкурентів незалежно від того, чи стосувалися вони запитань конфіденційного характеру чи ні.

У ході вивчення і дослідження джерел інформації проводиться їх оцінювання з позиції надійності та достовірності одержуваної з них інформації. Оцінювання джерел інформації здійснюється методом ранжирування (класифікації) самих джерел, з яких надходить інформація. У більшості випадків може використовуватися система експертної оцінки (безпосередньо аналітиком) надійності та достовірності отриманих даних. Рівень підготовки та практичні навички дозволяють співробітнику аналітичного підрозділу найбільш точно оцінити власне інформацію, її джерело і спосіб її отримання.

У процесі оцінювання достовірності інформації та її джерела необхідно враховувати можливість навмисної дезінформації, а також отримання ненавмисно спотвореної інформації. В обох випадках необхідно проведення додаткової перевірки і більш докладного всебічного аналізу отриманої інформації для прийняття рішення про її викорис-

тання у ході аналітичних досліджень. З урахуванням результатів оцінювання отриманої інформації, а також джерел та способів її отримання здійснюються збір і узагальнення (систематизація) необхідних для проведення повноцінного аналізу відомостей. У ході третього етапу аналітичної роботи проводиться повноцінний аналіз отриманої інформації і, на основі його результатів, – всебічний аналіз стану системи захисту інформації, виробляються ефективні заходи щодо її вдосконалення. На цьому етапі оформляються результати аналітичних досліджень, готуються висновки, рекомендації та пропозиції в галузі захисту інформації, яка охороняється.

Аналіз стану системи захисту інформації включає вивчення можливих каналів витоку інформації, оцінювання ефективності заходів щодо їх закриття, оцінювання дій персоналу підприємства за рішенням завдань у сфері захисту інформації, визначення основних напрямків діяльності щодо захисту інформації.

Зміст і основні види аналітичних звітів. Основною формою представлення результатів аналітичних досліджень є аналітичний звіт. Звіти можуть оформлятися в письмовому вигляді, також вони можуть бути представлені в усній формі, супроводжуватися графіками, діаграмами, малюнками, таблицями, які пояснюють або відбивають результати проведеної роботи. Основні розділи аналітичного звіту наступні: цілі і завдання аналітичного дослідження (цілі та задачі аналітичного дослідження, шляхи вирішення поставлених завдань, питання, що підлягають аналізу та оцінювання; передбачувані результати дослідження); джерела інформації, ступінь достовірності отриманої інформації (оцінки отриманої інформації, джерел і способів її отримання, результати аналізу ступеня достовірності отриманої з використанням цих джерел аналітичної інформації); узагальнення отриманої інформації (алгоритм збору й узагальнення необхідної для проведення повноцінного аналізу інформації – з усього обсягу отриманої та обробленої інформації виділяються найбільш значущі факти); основні й альтернативні версії чи гіпотези (мотивоване розподіл версій, що пояснюють або характеризують досліджувані події і факти, на основну та додаткові або альтернативні); відсутня інформація (додаткова інформація, необхідна для підтвердження основної версії, її джерела та способи її отримання); висновок, висновки (результати аналізу та оцінювання поставлених питань, висновки про ступінь важливості отриманої та обробленої інформації, значення цієї інформації для прийняття конкретних рішень у сфері захисту конфіденційної інформації, взаємозв'язок результатів цього аналітичного дослідження з іншими напрямками аналітичної роботи у сфері захисту інформації, можливі загрози захищаються, а також можливі наслідки впливу негативних факторів); пропозиції та рекомендації щодо вдосконалення роботи в області захисту інформації (конкретні пропозиції та рекомендації керівництву підприємства та керівникам структурних підрозділів щодо вдосконалення роботи в галузі захисту конфіденційної інформації; вироблені на основі проведеного аналізу отриманої інформації, а також різних подій і фактів конкретні заходи, прийняття яких необхідно для закриття можливих каналів витоку інформації та запобігання потенційних загроз захищається). В окремих випадках, на основі результатів проведення більш глибокого аналізу стану системи захисту інформації виробляються алгоритм і способи дій персоналу підприємства в конкретних ситуаціях. Залежно від призначення використовуються такі основні види аналітичних звітів: оперативний (тактичний) звіт; перспективний (стратегічний) звіт; періодичний звіт.

Оперативні (тактичні) звіти відображають результати аналітичних досліджень, проведених для підготовки і прийняття будь-якого оперативного (екстреного) рішення з питання короткочасного (термінового) характеру. У ході проведення таких досліджень аналізу та оцінці піддається інформація, переважно, невеликого обсягу. Перспективні (стратегічні) звіти містять інформацію, більш повну за змістом. Аналіз цієї інформації не обмежений терміном (часом) його проведення. У такі звіти, здебільшого, включається інформація, що містить більш повний аналіз передумов конкретних ситуацій, фактів, по-

дій. У звітах викладаються прогнози та перспективи розвитку цих ситуацій. Звіти цього виду відповідають постійним напрямками аналітичних досліджень. Періодичні звіти призначені для аналізу стану системи захисту інформації (окремих напрямків захисту інформації) відповідно до розробленого та затвердженого керівництвом підприємства графіком. Ці звітів не залежать від подій (виникнення різних ситуацій), пов'язаних із захистом інформації. Такі звіти готуються з проблем (напрямків), що є об'єктами постійної уваги з боку служби безпеки підприємства (його аналітичного підрозділу).

До складання звітів, незалежно від форми їх подання, пред'являються загальні вимоги, такі як: наявність глибокого аналізу подій (фактів, отриманої інформації), простота, чіткість і грамотність викладу матеріалу, логічність наведених міркувань і висновків, відповідність звітів встановленою формою. Одне з найбільш важливих вимог, що висуваються до звітів, полягає в тому, що їх зміст і рівень підготовки аналітичного матеріалу повинні відповідати запитам конкретних споживачів аналітичної інформації – керівників структурних підрозділів або окремих співробітників підприємства.

Класифікація методів аналізу інформації. Повнота та якість проведення аналітичних досліджень, достовірність отриманих результатів і ефективність вироблених пропозицій та рекомендацій великою мірою залежать від тих методів аналізу інформації, які були вибрані і використовувалися співробітниками аналітичного підрозділу безпосередньо у ході проведення досліджень.

Висновки і пропозиції. Проведення аналітичної роботи в галузі захисту інформації дозволяє оцінити або переоцінити рівень поточного стану інформаційної безпеки підприємства, виробити рекомендації щодо забезпечення (підвищенню) інформаційної безпеки підприємства, знизити потенційні втрати підприємства чи організації через підвищення стійкості функціонування корпоративної мережі, розробити концепцію та політику безпеки підприємства, а також запропонувати плани захисту конфіденційної інформації підприємства, що передається по відкритих каналах зв'язку, захисту інформації підприємства від навмисного спотворення (руйнування), несанкціонованого доступу до неї, її копіювання чи використання.

Список використаних джерел

1. *Домарев В. В.* Защита информации и безопасность компьютерных систем / В. В. Домарев. – К. : Диасофт, 1999. – 480 с.
2. *Концепція* технічного захисту інформації в галузі зв'язку України [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua.
3. *Про державну* таємницю [Електронний ресурс] : Закон України від 21.09.1999 р. № 1079-XIV. – Режим доступу : http://dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=88291&cat_id=38828.
4. *Тардаскін М. Ф.* Технічний захист комерційної таємниці підприємства зв'язку : навч. посіб. / *М. Ф. Тардаскін;* за ред. М. В. Захарченка, М. Ф. Тардаскін, В. Г. Кононович. – Одеса : ОНАЗ, 2002. – 76 с.
5. *Ткач Ю. М.* Окремі аспекти інформаційно-аналітичної діяльності у процесі навчання математики фахівців з інформаційної безпеки / Ю. М. Ткач / Дидактика математики: проблеми і дослідження : міжнародний збірник робіт. – Донецьк, 2013. – Вип. 40. – С. 151–158.