7. ECONOMIC SECURITY OF BUSINESS ENTITIES

Bashynska I.
PhD in economic sciences
Odessa national polytechnic university, Odessa, Ukraine

INFORMATION SECURITY OF TRADE SECRETS OF INDUSTRIAL ENTERPRISES

Башинська І.О.
к.е.н., старший викладач кафедри обліку, аналізу та аудиту
Одеський національний політехнічний університет, м. Одеса,

ІНФОРМАЦІЙНА БЕЗПЕКА КОМЕРЦІЙНОЇ ТАЄМНИЦІ ПРОМИСЛОВИХ ПІДПРИЄМСТВ

Для забезпечення інформаційної безпеки комерційної таємниці запропоновано використання комплексного підходу, а саме – аудиту інформаційної безпеки. Аудит дозволить виявити канали витоку, оцінити їх критичність і ймовірність витоку по ним. Аналіз даних, зібраних під час аудиту, дасть можливість вибору засобів контролю каналів, виходячи з бізнес-моделі підприємства і типів каналів. Розглянуто основні складові експертизи (аудиту) інформаційної безпеки: аудит інформаційної безпеки, аудит програмного забезпечення, аудит інформаційної системи. Визначено практичну значимість звіту з аудиту для промислових підприємств.

Ключевые слова: *інформаційна безпека, комерційна таємниця, промислові підприємства, аудит, експертиза.*

In the article offered the use of an integrated approach - namely, audit of information to ensure information security of trade secret. The audit will identify leakage; assess their criticality and probability of leakage on them. Analysis of data collected during the audit will enable the choice of control channels based on the business model of the enterprise and channel types. The main components of the examination (audit) information security: information security audit, audit software audit information system. Practical significance of the report of the audit for the industrial enterprises is defined

Key words: *information security, trade secrets, industrial enterprises, the audit, the examination.*

На сьогоднішній день інформаційна сфера є ведучою в діяльності держави і чинить вплив на всі елементи функціонування промислових підприємств. В сучасних умовах зростаючої конкуренції підприємства шукають нові шляхи і можливості підвищення своєї конкурентоспроможності. Особливо це стосується підприємств, що зайняті у сфері продажу товарів, адже, тут конкуренція найбільш висока і відчутна. Діяльність промислових підприємств потребує особової уваги щодо забезпечення охорони своїх об’єктів, персоналу та інтелектуальної власності. Все це робить питання посилення безпеки цифрових мереж та інфраструктур особливо актуальним [1; 2].

Інформація, яку використовують у підприємницькій діяльності, вельми різноманітна. Її можна поділити на два види: промислова і комерційна. До промислової належать: інформація про технологію і спосіб виробництва, технічні відкриття і винаходи; «ноу-хау»; конструкторська документація, програмне забезпечення тощо.

Комерційна інформація – це відомості про фінансово-економічне становище підприємства (бухгалтерська звітність), кредити і банківські операції, про укладені договори, контрагентів, структуру капіталів і плани інвестицій, стратегічні плани маркетингу, аналіз конкурентоспроможності власної продукції, клієнтів, плани виробничого розвитку, ділове листування та ін. [3] Комерційна таємниця підприємства – це інформація, що не є державним секретом і пов'язана з виробництвом, технологічною інформацією, управлінням, фінансами та ін. Така загальна характеристика категорії «комерційна таємниця» підприємства є законодавчо правильною. Розголошування (передача, витік) її може завдати збитку інтересам підприємства.

В першу чергу необхідно визначити канали витоку інформації і засоби їх контролю, а, при необхідності, і перекриття. Найважливішим інструментом в цьому є аудит інформаційної

безпеки. Аудит дозволить виявити канали витоку, оцінити їх критичність і ймовірність витоку по ним. Аналіз даних, зібраних під час аудиту, дасть можливість вибору засобів контролю каналів, виходячи з бізнес-моделі підприємства і типів каналів [4].

Експертиза інформаційної безпеки комерційної таємниці повинен забезпечуватися з трьох боків (рис. 1).

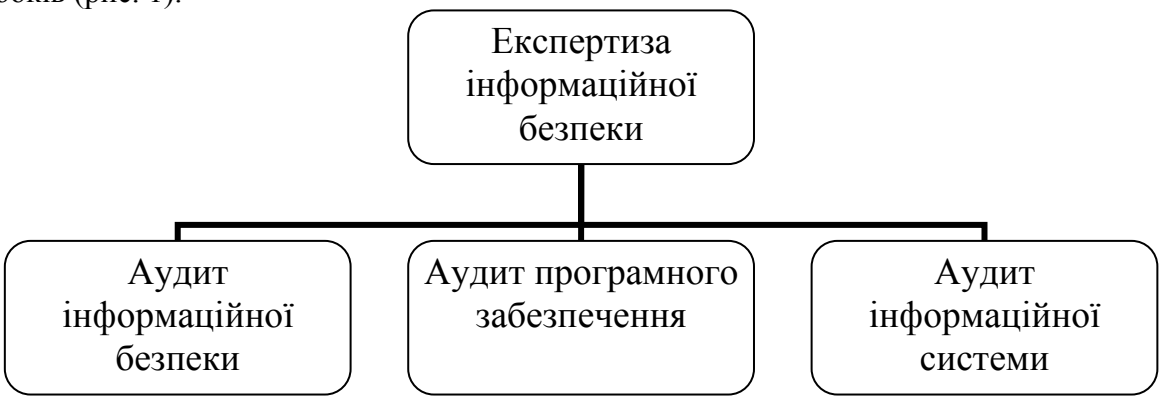

Рис. 1. Складові експертизи інформаційної безпеки

1. Аудит інформаційної безпеки – незалежна експертна оцінка захищеності інформаційної системи компанії з урахуванням таких факторів як персонал, процеси і технології. Основною метою аудиту є визначення відповідності застосовуваних в організації захисних заходів обраними критеріями інформаційної безпеки.

Результат аудиту – це аналіз відповідності вимог бізнесу поточному рівню зрілості IT-інфраструктури, виражений у вигляді звіту.

2. *Аудит програмного забезпечення* – це перевірка використання промисловим підприємством легального програмного забезпечення.

3. *Аудит інформаційної системи* – це оцінка об'єктивних даних про поточний стан обчислювальної і телекомунікаційної структури, її відповідності стандартам, а також вимогам керівництва компанії. На сьогоднішній день подальший розвиток компаній залежить від оптимальної роботи IT-інфраструктури, у зв'язку з цим в її організацію і розвиток вкладається все більше і більше ресурсів.

Основною проблемою, з якою стикаються промислові підприємства – це нерозуміння цілей бізнесу управлінням IT-підрозділу. Це призводить до того що завдання, які вирішуються IT-підрозділ не корелюють з цілями компанії і виникає конфлікт.

Що практично може дати звіт з аудиту промисловим підприємствам?

Звіт надає повну картину інформаційної системи компанії:

- повну картину серверів, робочих станцій, мобільних пристроїв, мережевого обладнання, які ролі виконують сервера, які потужності і ресурси виділені під сервера, що полегшує інвентаризацію і вносить ясність в капіталовкладення, дозволяє прогнозувати і ефективно коригувати бюджет.
- замовник бачить всі ділянки, об'єкти і канали передачі інформації в компанії, схему передачі, обробки та зберігання інформації в компанії, може керувати інформацією в бізнес-процесах, організовувати захист передачі даних, безпечне зберігання і резервне копіювання комерційної інформації.

Звіт описує програмне забезпечення, що використовується в компанії:

- замовник бачить все програмне забезпечення (ПЗ), встановлене в компанії, бачить програми, що використовуються в роботі, приймає рішення про економію коштів на програмне забезпечення, відмовившись від дорогих програм або замінивши їх безкоштовними аналогами. Розташовуючи подібною інформацією можна коректно оцінити необхідність фінансових вкладень в ПО, оптимізувати витрати, підібравши оптимальну схему ліцензування.

Звіт описує інформаційні інструменти та бізнес-процеси компанії:

- вироблятися аналіз нормативно-правової бази, внутрішніх документів і регламентів прийнятих в компанії по роботі з комерційною інформацією.
- складається карта основних бізнес-процесів в роботі ІТ, що прямо впливають на заходи щодо захисту інформації.
- виділяється основні проблеми при взаємодії ІТ та бізнесу, присвоюється рівень моделі зрілості ІТ компанії, визначаються здібності процесів ІТ.
- досліджуються інформаційні інструменти, визначається їх ефективність і пропонується оптимізувати їх або замінити на більш дієві.
- дозволяє зрозуміти рівень захищеності від крадіжки своїх платіжних інструментів, такі як клієнт-банк.
- дозволяє підвищити продуктивність і гнучкість інструментів бухгалтерського та управлінського обліку, таких як 1С.
- розширює функціональність і контроль інструментів внутрішнього документообігу та відпрацювання доручень.
- дозволяє впровадити нові інструменти для підвищення продуктивності праці та полегшення виконання завдань у колективній діяльності, наприклад, корпоративні засоби спілкування (захищені телефонія і обмін текстовими повідомленнями).

Таким чином, експертиза (аудит) інформаційної діяльності наводить повну картину стану інформаційної системи промислового підприємства зі знайденими проблемами та рекомендаціями щодо їх усунення.

Литература:

1. Башинська І.О. Розділ 4.2. Сучасні засоби забезпечення інформаційної складової економічної безпеки промислового підприємства (С. 310-315) у кол. монографії «Формування механізму стійкого розвитку економіки: теорія та практика» – Дніпропетровськ: «ФОП Дробязко С.І.», 2014. – 438 с.
2. Filippova S. World experience in creation the corporate sales manual as internal instrument of marketing communications of industrial enterprise / Bashynskaya Irina, Filippova Svetlana // Вісник ТНЕУ. – 2012. – №5-2. – С. 234-240
3. Конспект лекцій з дисципліни «Інформаційно-аналітичне забезпечення економічної безпеки» для студентів Інституту бізнесу, економіки та інформаційних технологій (ІБЕІТ) денної та заочної форми навчання за спеціальністю 8.18010014 – «Управління фінансово-економічною безпекою» /Уклад.: Башинська І.О. – Одеса: ОНПУ, 2014. – 207 с. (ел. версія, рег. КЛ05549 от 28.04.2014 г. № 2031-РС-2014)
4. Bashynska I. Ensuring economic security of modern enterprise as a systematic approach // British Journal of Science, Education and Culture, 2014, No.1. (5) (January-June). Volume IV. “London University Press”. London, 2014. – 804 p. – P. 340-343

Melnik H.A.

THEORETICAL ASPECTS OF THE CONTROLLING SYSTEM OF ECONOMIC SECURITY

Мельник Е.А.

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ФОРМИРОВАНИЯ СИСТЕМЫ КОНТРОЛЛИНГА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

В статье рассмотрены вопросы формирования системы контроллинга экономической безопасности предприятия

***Ключевые слова**: контроллинг экономической безопасности, система, алгоритм.*

The article discusses the formation of a controlling system of economic security

***Keywords:** kontrolling of economic security, system, algorithm.*

С развитием рыночных экономических отношений в Украине значительно изменились экономические приоритеты. Современная рыночная среда характеризуется