Онищенко Світлана,
доктор економічних наук, професор,
Глушко Аліна,
кандидат економічних наук, доцент,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БІЗНЕСУ В СУЧАСНИХ УМОВАХ

Ключові слова: інформація, інформаційна безпека, діджиталізація, захист інформації.

Svitlana Onyshchenko,
Doctor of Economics, Professor,
Alina Hlushko,
PhD in Economics, Assistant Professor
National University «Yuri Kondratyuk Poltava Polytechnic»

IMPROVING THE LEVEL OF INFORMATION SECURITY OF BUSINESS IN MODERN CONDITIONS

Key words: information, information security, digitalization, information protection.

В умовах інформаційно-технологічного розвитку, що характеризується, з одного боку, інтенсифікацією використання сучасних інформаційних технологій в усіх галузях національної економіки, а з іншого, збільшенням масштабів та частоти кібератак, появою нових ризиків і загроз безпеці суб'єктів господарювання та держави в цілому, питання підвищення рівня інформаційної безпеки набуває особливої актуальності.Відзначаючи роль та значення існуючих наукових досліджень із питань інформаційної безпеки, цілком очевидно, що в умовах інтенсифікації процесів інформатизації та прогресивного розвитку IT-сфери однією з найбільш актуальних проблем є проблема кібератак, що зумовлює необхідність підвищення захисту інформації.

Інформаційна безпека суб'єктів господарювання характеризує стан їх доступу до інформації, її захищеності, зберігання, ефективності використання, проведення ділової розвідки, інформаційно-аналітичної роботи із зовнішніми та внутрішніми суб'єктами, здатність інформаційно-аналітичної системи суб'єктів господарювання до розвитку. Забезпечення інформаційної безпеки суб'єктів господарювання полягає в своєчасному виявленні каналів втрат інформації, загроз та рівня їх важливості, типів суб'єктів викрадення інформації, способів їх дій; оперативному реагуванні на загрози; створення умов для максимально можливого відшкодування збитку; уникненні економічного та промислового шпіонажу.

Отже, інформаційна безпека підприємств покликана захистити їх інтереси та їх персоналу від неправомірного використання внутрішньої інформації та

охорону комерційної таємниці, яка нерідко становить вагому частку інтелектуальної власності суб'єкта бізнесу.

Однак, незважаючи на намагання оберегти комерційну таємницю та інші джерела інформації, часто трапляється явище, коли інформація розповсюджується особами, які не мають на це жодних прав. В сучасних умовах ведення бізнесу таке явище є достатньо розповсюдженим, оскільки саме інформація щодо ноу-хау, технологій, методів ведення діяльності та управління окремими бізнес-процесами формує конкурентоспроможність багатьох суб'єктів господарювання. А в умовах постійної конкуренції навіть краплина потрібної інформації може кардинально змінити ринкові умови для окремого суб'єкта бізнесу, а для іншого – навпаки обернутись втратами та збитком. Саме тому, у країнах Західної Європи та США 20 % втрати конфіденційної інформації може призвести до банкрутства підприємства [1].

Сучасна залежність підприємств від інформаційних систем та їх послуг означає, що суб'єкти господарювання стають усе більше уразливі до загроз інформаційної безпеки. Взаємодія суспільних і приватних мереж, а також спільне використання інформаційних ресурсів збільшує труднощі управління доступом та забезпечення гарантій послуг і безпеки інформаційно-комунікаційних систем та мереж.

Активізація процесів діджиталізації господарської діяльності створює передумови для зростання випадків несанкціонованого використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [2], тобто кіберзлочинності.

Ще в 90-ті роки у Сполучених Штатах Америки комп'ютерні шахрайства щорічно спричиняли збитки на суму понад $10 млрд [3]. У Великій Британії, де комп'ютерна злочинність на той час зросла в 4 рази, за оцінками Конфедерації британських промисловців, щорічні збитки сягали 5 млрд. фунтів стерлінгів.

Нині фінансові втрати від кіберзлочинності щороку зростають. Згідно з даними дослідження, проведеного експертами Центру стратегічних і міжнародних досліджень (CSIS) та компанії McAfee, що займається розробкою антивірусного програмного забезпечення, рівень втрат від кіберзлочинів у світовій економіці зростає серйозними темпами: якщо в 2014 році вони становили 345-445 млрд. доларів (0,6% світового ВВП), то в 2016 році вже 445-600 млрд. доларів (08% світового ВВП), в 2017 році – близько 1,5 трильйона доларів. Світові збитки лише від хакерської атаки за допомогою вірусної програми NotPetya склали 850 млн. доларів, з них 300 млн. доларів – фінансові втрати національної економіки України (0,4 % ВВП) [4]. Хакерські атаки протягом 2020 року коштували світовій економіці понад трильйон доларів або 820 мільярдів євро, що на 50 відсотків вище, ніж у 2018 році.

Встановити реальні масштаби фінансових втрат від дій кіберзлочинців надзвичайно складно і майже неможливо. Проте відсутність офіційної статистики не зменшує актуальність та важливість завдання забезпечення безпеки інформації. Адже саме інформація є одним з універсальних видів ресурсів, які необхідні як для процесу прийняття рішень, так і для формулювання стратегічних, тактичних та оперативних задач господарського розвитку на макро- , мезо- та мікрорівнях.

Ключовим моментом захисту від кіберзлочинності є підготовка і виявлення вразливих місць, а також стійкість з точки зору взаємодії з загальними системами управління.

Основоположними в сфері управління інформаційною безпекою є Міжнародні стандарти ISO/IEC 27001 та ISO/IEC 27002 (мав назву ISO/IEC 17799 до 2007 року). Вони представляють собою модель системи менеджменту, яка визначає загальну організацію процесів, класифікацію даних, системи доступу, напрямки планування, відповідальність співробітників, використання оцінки ризику і т. ін. в контексті інформаційної безпеки. Так, завдяки впровадженню стандарту ISO/IEC 27001 суб'єкти господарювання отримали можливість оцінювати свої ризики, впроваджувати засоби контролю щодо їх пом'якшення, здійснювати контроль за ризиками, покращуючи, за необхідності, захист інформації. Стандарт ISO/IEC 27002 використовується для встановлення системи ефективного інформаційного захисту та удосконалення методів інформаційного захисту.

На сьогоднішній день існує понад 40 міжнародних стандартів серії ISO/IEC 27000, що охоплюють все: від створення спільного словника (ISO/IEC 27000), управління ризиками (ISO/IEC 27005), безпеки у хмарних технологіях (ISO/IEC 27017 і ISO/IEC 27018) до методів судової експертизи, що використовують для аналізу цифрових доказів та розслідування інцидентів ISO/ IEC 27042 та ISO/IEC 27043 відповідно) [5]. Вони дають можливість підприємствам постійно оновлюватися у боротьбі з кіберзлочинністю.

Таким чином, зміцнення інформаційної безпеки підприємств ґрунтується на забезпеченні достовірності, конфіденційності, цілісності інформаційних ресурсів. Побудова ефективної системи управління інформаційною безпекою на базі міжнародних стандартів серії ISO в сучасних інформаційно-комунікаційних системах і мережах є важливим завданням для кожного суб'єкта господарювання.

Список використаних джерел

1. Кавун С.В., Пилипенко А.А., Ріпка Д.О. Економічна та інформаційна безпека підприємств у системі консолідованої інформації: навч. посіб. Харків: Вид. ХНЕУ, 2013. 364 с..

2. Онищенко С.В., Глушко А.Д. Концептуальні засади інформаційної безпеки національної економіки в умовах діджиталізації // Соціальна економіка. ХНУ, 2020. Вип. 59. с. 14-24.

3. Живко З., Живко М., Ортинський В., Керницький І. Економічна безпека підприємств, організацій та установ. Підручник. Алерта, 2009. 544 с.

4. Economic Impact of Cybercrime – No Slowing Down. Report of the Center for Strategic and International Studies (CSIS), 2018.Homepagehttps://www.csis.org/analysis/economic-impact-cybercrime.

5. Official site the International Organization for Standardization Homepage https://www.iso.org/home.html.