Менеджмент

УДК: 681.3.06

**Полянська Алла Степанівна**
*доктор економічних наук, професор*
*Івано-Франківський національний технічний університет нафти і газу*
**Polyanska Alla**
*Doctor of Economics, Professor*
*Ivano-Frankivsk National Technical University of Oil and Gas*
*ORCID: 0000-0001-5169-1866*

**Дюк Оксана Михайлівна**
*доктор філософії з менеджменту*
*Івано-Франківський національний технічний університет нафти і газу*
**Diuk Oksana**
*PhD of Management*
*Ivano-Frankivsk National Technical University of Oil and Gas*
*ORCID: 0000-0002-5819-144X*

# ФОРМУВАННЯ МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ
# FORMATION OF THE MODEL FOR PROVIDING INFORMATION PROTECTION AT THE ENTERPRISE

***Анотація.*** *Проведено дослідження передумов формування моделі забезпечення захисту інформації на підприємстві. Охарактеризовано складові даної моделі на основі виділення таких складових як стратегія і організація діяльності, технологія, люди, процеси. Обґрунтовано, що їх врахування сприятиме прискоренню комплексного впровадження і підтримки працездатності цілісної системи інформаційної безпеки, що погоджує правові, адміністративні, організаційні, технологічні, науково-*

*технічні і фізичні заходи захисту інформації. Підкреслено, що менеджери з інформаційної безпеки виконують ключову роль у забезпеченні інформаційної безпеки, виконуючи відповідну роботу та взаємодіючи у межах сформованої інфраструктури та центрів інформаційної відповідальності. Підсумовано, що розглянута модель захисту інформації на підприємстві охоплює фактори внутрішнього середовища, які на рівні окремого суб'єкта господарювання дозволяють створити систему інформаційного захисту, інтегруючи елементи розглянутої моделі, що забезпечують інформаційний захист, у систему управління підприємством.*

***Ключові слова:*** *інформація, захист інформації, інформаційна безпека, підприємство, модель.*

***Summary.*** *Information security of an enterprise is a functional element of the system for ensuring its strategic development. Its main task is to ensure the stability of the enterprise's existence in the present and the prospects for its sustainable development in the future. The integrated system for ensuring the information security of enterprises takes into account modern legal and organizational and managerial measures, as well as software and hardware tools for countering external and internal threats, which ensures the state of information security and the prospects for the development of information technologies. The organizational level of information protection includes organizational regulation, organizational regulation and organizational instruction and ensures the organization of security, regime, work with personnel, with documents, standards for the use of technical security means and procedures for information and analytical activities of the enterprise to identify threats. The organizational aspect of ensuring the information security of an enterprise is one of its most important elements, since the effectiveness of all activities to support the information security system at the proper level largely depends on the actions taken for implementation. The main task is to characterize the information*

*security system at the enterprise. The research of the information security system at the enterprise was carried out. It has been determined that the correct solution to the issue of creating information security bodies will help accelerate the integrated implementation and maintenance of an integral information security system, coordinate legal, administrative, organizational, technological, scientific, technical and physical measures to protect information. It is given that information security programs should take into account how an organization and its people, processes and technologies interact; and how organizational governance, culture, human factors, and architecture support or hinder an enterprise's ability to protect information and manage risk. It is highlighted that information security managers should do their best to create programs that meet the goals and priorities of the enterprise, benefit the enterprise and support the ability of management to innovate while controlling risks.*

***Key word:*** *information, information protection, information security, enterprise, model*

**Постановка проблеми.** В епоху глобальної економіки, постійно мінливих корпоративних ризиків відбувся вагомий вплив світової пандемії COVID-19 на соціально-економічний розвиток кожної країни світу. Вірусна небезпека стала викликом не тільки для системи охорони здоров'я, а й створила передумови для ефективного ведення бізнесу, залишаючи позаду такі бар'єри як кордони. Ділова активність під час пандемії пришвидшила процеси цифровізації, зокрема глобальна ізоляція населення у всьому світі призвела до значного збільшення користувачів мережі Internet. Швидке входження суспільств в кіберпростір призвело до нових викликів для системи інформаційної безпеки. Інформаційна безпека перетворилась у важливий фактор, що сприяє розвитку бізнесу. Результати досліджень та їх постійне появою нових стандартів, інструментів і технологій щодо забезпечення інформаційної безпеки є передумовою для формування

механізмів, що допомагають захистити організаціям бізнес-транзакції, а також інфраструктуру та інформацію. Проте вітчизняним підприємствам на сьогодні складно відповідати нормативним вимогам інформаційної безпеки, забезпечуючи належні економічні умови діяльності та управління ризиками. Ключова роль інформаційної безпеки досі чітко не визначена в багатьох організаціях попри те, що окремі організації розглядають інформаційну безпеку як центр витрат. Слід зазначити, що ефективно керовані організації щодо інформаційної безпеки використовують цю перевагу у досягненні бізнес-цілей за рахунок врахування загроз та зменшення вразливості.

Суттєвим недоліком у діяльності підприємств сьогодні є те, що вони часто розглядають інформаційну безпеку ізольовано, вважаючи, що безпека – це чиясь відповідальність, звідси недостатність спільних зусиль, щоб пов'язати програму інформаційної безпеки з бізнес-цілями. Такий підхід легко може привести до виникнення слабких місць в управлінні безпекою та до появи серйозних порушень. З фінансової точки зору така ситуація може привести до непродуктивних витрат, а з операційної точки зору заходи щодо забезпечення інформаційної безпеки можуть не принести очікуваного зиску для бізнесу, що призведе до виникнення ризику для інформації.

Враховуючи викладене вище, зазначимо, що основними завданнями для сучасних підприємств є забезпечення безпеки економічної інформації та створення надійної моделі кібернетичної безпеки для своєчасного виявлення, запобігання та нейтралізації реальних і потенційних загроз та викликів, попередження кібернетичних втручань та формування цифрових систем управління безпекою, що є актуальністю сьогодення [6].

**Аналіз основних досліджень і публікацій.** Проблема дослідження системи забезпечення захисту інформації на підприємстві на сьогоднішній день набуває значної актуальності в роботах вітчизняних та зарубіжних вчених, зокрема Близнюк І. М., Братель О. Р., Бондаренко В. О., Бучило І. Л., Горбатюк О. М., Гуцалюк М. О., Ляшенко О. М., Камлик М. І., Козаченко

Г. В., Остроухов В. В., Пономарьов В. П., а також такі зарубіжні автори, як Chang H., Kim J., Lim S., Horn A., Tawileh A., Hilton J. та інших.

**Мета статті.** Метою статті є дослідження передумов створення моделі забезпечення захисту інформації на підприємстві, характеристика складових даної моделі із виділенням її організаційного аспекту.

**Виклад основного матеріалу дослідження.** Інформаційну безпеку більшою мірою пов'язують із виключно технічним завданням. ІТ-служби створюють технології, необхідні для захисту інформації, але самі по собі технології не є рішенням. Для захисту інформації підприємствам необхідно розробити політику інформаційної безпеки, яка підтримується стандартами, процедурами і керівними принципами. Менеджмент підприємства в особі керівників та фахівців визначає цілі, завдання та напрями програми інформаційної безпеки і очікування щодо того як, ким, коли і де інформація може використовуватися, зокрема спільно, передаватися і знищуватися. На багатьох підприємствах стратегії, політика, процеси і стандарти інформаційної безпеки розробляються без врахування того, як організаційна культура впливає на ефективність реалізації програм захисту. Зусилля щодо забезпечення безпеки, які не враховують поведінку людей і їх реакцію на технології захисту та їх використання, часто не приносять очікуваних вигод.

Програми інформаційної безпеки повинні враховувати, як організація та її люди, процеси та технології взаємодіють, і як організаційне управління, культура, людський фактор і технології інформаційного захисту підтримують або перешкоджають здатності підприємства захищати інформацію і управляти ризиками. Звідси серед завдань керівництва у сфері інформаційної безпеки важливо створити програми, що відповідають цілям і пріоритетам підприємства, містять конкретні види діяльності, що потребують захисту, описують способи їх забезпечення, формують можливість створення іміджу та зв'язків із зовнішнім середовищем,

підтримують здатність менеджменту реалізувати необхідні зміни при одночасному контролі ризиків.

Розробка програми інформаційної безпеки та її інтеграція в бізнес-цілі, завдання, стратегії і дії ускладнюються відсутністю моделі, яка враховувала б і охоплювала види і напрями робіт, які забезпечують інформаційну безпеку. Мова йде про концептуальну модель, яку керівники бізнес-підрозділів і фахівці з інформаційної безпеки можуть використовувати для опису і роз'яснення користувачам з доступом до інформації шляхів досягнення інформаційної безпеки в бізнесі, і не тільки як користувачів технічних засобів.

Беззаперечним є те, що підприємства стають все більш залежними від IT сфери для пришвидшення, здешевлення та оптимізації бізнес-операцій. В сучасних умовах економіки, заснованої на знаннях, інформація має вирішальне значення для здатності підприємства не тільки виживати, але й процвітати. Досвідчені керівники підприємств знають, що інформація заслуговує, принаймні, того ж рівня захисту, що і будь-який інший актив, звідси і поява менеджерів з інформаційної безпеки стає звичайним напрямом організаційних змін на підприємствах. Однак поява фахівця з інформаційної безпеки повною мірою не вирішує завдання захисту інформаційного простору підприємства. Ключову роль, яку відіграє менеджер з інформаційної безпеки – це будівництво міцної та непорушної системи безпеки підприємства, яка зможе функціонувати на підприємстві, організовуючи захист власності, інформації, ресурсів та взаємодіяти із зовнішнім середовищем, обмінюватись інформацією, приваблювати споживачів, задовольняти інформаційні потреби стейкхолдерів. Звідси, менеджер з інформаційної безпеки має бути добре обізнаним у питаннях ринкової економіки, вміти швидко зреагувати на зміни кон'юнктури ринку, розуміти усі аспекти ділових відносин тощо [8]. Для досягнення мети своєї

діяльності, що гармонізована із цілями і завданнями підприємства загалом, менеджер з інформаційної проводить свою роботу у таких напрямах:

- удосконалення організаційно-правових засад інформаційного забезпечення роботи підприємства;
- організація роботи служби безпеки, яка має на меті захистити інтереси підприємства та працівників;
- встановлення взаємозв'язку із системою економічної та фінансової безпеки, що закріплює збалансованість і мобільність до макро- та мікрозмін;
- проведення оцінки ризику у сфері інформаційної безпеки;
- взаємодія з органами державної влади, що має регулюючий характер [7].

Попри це, менеджери з інформаційної безпеки стикаються з безліччю проблем, включаючи зміну профілів ризиків, недоліками фінансування, культурними проблемами, а також внутрішніми слабкими сторонами своєї діяльності і зовнішніми загрозами. Управління інформаційною безпекою ніколи не було настільки важливим як сьогодні, проте досвід діяльності у даній сфері пропонує досить незначний перелік формальних моделей, які б могли допомогти менеджеру з інформаційної безпеки робити свою роботу більш ефективно. А у небагатьох існуючих моделей не враховується, як і що потрібно змінювати для забезпечення інформаційної безпеки на підприємствах, як доцільно розвивати корпоративну культуру для реалізації необхідних змін, і які результати потенційно матиме підприємство від застосування таких моделей.

Інформаційна безпека підприємства є складовою системи управління його розвитком. Її основне завдання - забезпечити безпечне функціонування підприємства в поточному періоді та його сталий розвиток в майбутньому. Складова забезпечення інформаційної безпеки підприємств враховує сучасні організаційно-правові та адміністративно-управлінські заходи, а також програмно-технічні засоби протидії зовнішнім і внутрішнім загрозам,

що забезпечує стан захищеності інформації та перспективи розвитку інформаційних технологій [1-2].

Організаційно-правовий рівень захисту інформації включає правове забезпечення інформаційного захисту, організаційне регламентування, нормування, інструктування та організацію режиму охорони, роботу з кадрами, з документами, нормами використання технічних засобів безпеки та включає процедури інформаційно-аналітичної діяльності підприємства по виявленню загроз.

Заходи адміністративно-управлінського характеру щодо забезпечення інформаційної безпеки підприємства охоплюють інформування персоналу про правила роботи з конфіденційною інформацією, заходи відповідальності за порушення, процедури захисту і зберігання інформації, організацію охорони територій, створення відповідних організаційних структур щодо забезпечення безпеки інформаційних ресурсів, організацію конфіденційного діловодства підприємства тощо.

Попри те, що на сьогодні розроблено Стандарти з інформаційної безпеки [10], заходи щодо забезпечення інформаційної безпеки на підприємствах постійно розвивається, починаючи з криптографії на ранніх періодах контролю, створеного на основі розуміння того, що інформація є цінним активом. Зростання залежності від комп'ютерів для полегшення бізнес-операцій привела до удосконалення технологічних рішень з інформаційної безпеки, спрямованих на захист інформаційних інфраструктур підприємства від зовнішніх втручань. Однак, враховуючи те, що бізнес став розглядати інформацію як критично важливий актив і все більше використовувати загальнодоступні мережі для передачі конфіденційної інформації, питання захисту інформації попри розгляду удосконалення технологій такого захисту більше уваги почав приділяти стійкості самого підприємства [3-5].

Врахування зазначеного вище на рис. 1 пропонується модель захисту інформації на підприємстві, яка включає чотири елементи (рис. 1):

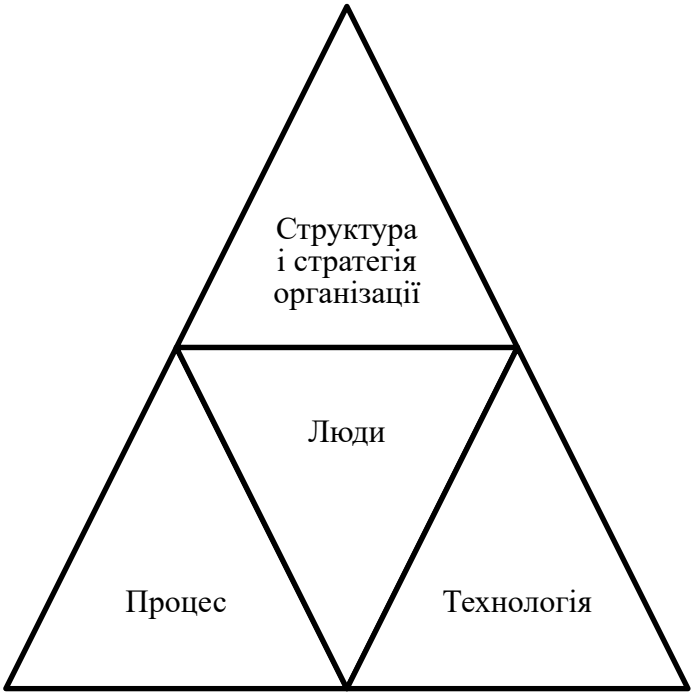


**Рис. 1. Елементи моделі захисту інформації на підприємстві**

1. Структура і стратегія організації: стратегія організація вимагає врахування елемента інформаційної безпеки та належної організації виконання відповідної роботи, що пов'язана із об'єднанням у мережі людей, активів і процесів, що взаємодіють один з одним в певних ролях і працюють для досягнення спільної мети.

2. Люди: людські ресурси і проблеми безпеки – два взаємопов'язані чинники, які визначають, хто реалізує відповідну стратегію, як і ким виконуватимуться положення стратегії інформаційної безпеки. Дана складова пропонованої моделі охоплює колективи працівників і враховує їх цінності, поведінку, готовність і упередження щодо забезпечення інформаційної безпеки. На рівні внутрішнього середовища для менеджера з інформаційної безпеки критично важливо працювати з такими питаннями, що пов'язані із людськими ресурсами:

– стратегії найму (доступ, перевірка біографічних даних, інтерв'ю, ролі і обов'язки);

– питання зайнятості (розташування офісу, доступ до інструментів і даних, навчання і обізнаність, переміщення по підприємству);

– припинення дії (причини звільнення, час догляду, ролі і обов'язки, доступ до систем, доступ до інших співробітників), робота із зовнішніми клієнтами, постачальниками, ЗМІ, зацікавленими сторонами та іншими особами, - діяльність, що може мати вагомий вплив на підприємство і повинна розглядатися в рамках поза безпеки.

3. Процес: врахування формальних і неформальних механізмів виконання завдань і забезпечення зв'язків з усіма видами робіт. Процеси ідентифікують, вимірюють, керують і контролюють ризики, доступність, цілісність та конфіденційність, а також забезпечують підзвітність, тобто формують центри інформаційної відповідальності, що виконують умови:

– відповідати стратегії, політиці та бізнес-вимогам підприємства;

– враховувати появу і та необхідність адаптації до мінливих вимог та викликів розвитку.

– відповідати належній формі та бути доступними до відповідного персоналу;

– періодично перевірятися за критерієм ефективності та результативності.

4. Технологія: складається з технічних інструментів, додатків та відповідної інфраструктури, які роблять процеси захисту інформації більш ефективними.

Таким чином, розглянута модель захисту інформації на підприємстві охоплює фактори внутрішнього середовища, які на рівні окремого суб'єкта господарювання дозволяють створити систему інформаційного захисту, інтегруючи елементи розглянутої моделі, що забезпечують інформаційний захист, у систему управління підприємством.

**Висновки і пропозиції.** Підсумовуючи викладене вище звернемо увагу на приклад Європи, де можна побачити, що формування моделі інформаційної безпеки – складний, довготривалий, багатофакторний та диверсифікований процес. Практичні дії та досвід сприяли становленню системи інформаційної безпеки, яке у європейських країнах проходило методично та цілеспрямовано, а також охоплювало різноманітні сфери діяльності, зокрема суспільну, господарську та державну. В Україні цей процес відбувається не системно, а нормотворча активність у сфері інформаційної безпеки активізувалася у 2014 році, до того ж з значним перегином у бік державної і суспільної інформаційної безпеки, а інформаційній безпеці підприємств приділено недостатньо уваги. Нові виклики 2019 – 2022 рр., а також особливості організації роботи щодо створення у системах управління підприємствами відповідних елементів привертають увагу до інформаційної безпеки, активізують нормотворчу діяльність у цій сфер, оптимізують методичне підґрунтя щодо посилення контролю за інформаційною безпекою, урегулюванням спірних моментів, посиленням протидії кіберзагрозам тощо [9]. Відтак, базуючись на сформованій системі інформаційної безпеки кожне підприємство може створити унікальну модель захисту інформації, враховуючи свої потреби, можливості, вимоги та розглянуті у статті організаційні аспекти такої моделі.

Організаційний аспект забезпечення інформаційної безпеки підприємства є одним з найважливіших її елементів, оскільки від прийнятих до реалізації дій, чітко визначених центрів інформаційної відповідальності, визначення зав'язків та взаємодії у забезпеченні інформаційної безпеки на підприємстві в значній мірі залежить ефективність всієї діяльності з підтримки системи інформаційної безпеки на належному рівні.

Слід зазначити, що обґрунтований підхід щодо підготовки фахівців у сфері інформаційної безпеки сприятиме прискоренню комплексного

впровадження життєздатних інформаційних систем підтримання безпеки на підприємствах та забезпечить працездатність системи управління на основі використання дієвих моделей захисту інформації, що враховуватимуть правові, адміністративні, організаційні, гуманітарні, технологічні, науково-технічні та фізичні заходи щодо захисту інформації.

**Література**

1. Chang H., Kim J., Lim S. Information security management system for SMB in ubiquitous computing. *Computational science and its applications - ICCSA 2006*. Berlin, Heidelberg, 2006. P. 707–715. doi: https://doi.org/10.1007/11751632_77 (date of access: 16.09.2022).
2. Horn A. Information security - more than an IT challenge for SME. URL: http://www.freshbusinessthinking.com/business_advice.php?CID=3&AID=2629&PGID3 (date of access: 16.09.2022).
3. Tawileh A., Hilton J., McIntosh S. Managing information security in small and medium sized enterprises: a holistic approach. *ISSE/SECURE 2007 securing electronic business processes*. Wiesbaden. P. 331–339. doi: https://doi.org/10.1007/978-3-8348-9418-2_35 (date of access: 16.09.2022).
4. Park J.Y., Robles R.J., Hong C.H., Yeo S.S., Kim T. IT Security Strategies for SME's, International Journal of Software Engineering and its Applications. 2008. 2(3), July. P. 91-98
5. McNally W., Tenner A. R., DeToro I. J. Total quality management. three steps to continuous improvement. *The journal of the operational research society*. 1993. Vol. 44, No. 1. P. 91. doi: https://doi.org/10.2307/2584442 (date of access: 16.09.2026).
6. Волот О. І. Інформаційна та кібернетична безпека сучасного підприємства: забезпечення та моделювання. *Центральноукраїнський науковий вісник. Економічні науки*. 2019. 3 (36). С. 238–247.

7. Донець Л., Ващенко Н. Економічна безпека підприємства: навч. посіб. Київ: Центр учб. літ., 2008. 240 с.
8. Перегіняк Н., Дюк О. Особливості діяльності сучасного менеджера безпеки. *Формування стратегії соціально-економічного розвитку підприємницьких структур в Україні*: матеріали Всеукр. науково-практ. інтернет-конф., м. Львів, 19–21 листоп. 2015 р. Львів, 2015. С. 168.
9. Бакай В. Й., Зима В. М. Нові виклики та особливості створення системи інформаційної безпеки підприємства. Вісник Хмельницького національного університету. Економічні науки. 2020. № 5. С. 19–22.
10. Стандарт інформаційної безпеки ISO / IEC 27002. URL: https://uk.wikipedia.org/wiki/ISO/IEC_27002 (дата звернення: 10.09.2022 р.).

**References**

1. Chang H., Kim J., Lim S. Information security management system for SMB in ubiquitous computing. *Computational science and its applications - ICCSA 2006*. Berlin, Heidelberg, 2006. P. 707–715. doi: https://doi.org/10.1007/11751632_77 (date of access: 16.09.2022).
2. Horn A. Information security - more than an IT challenge for SME. URL: http://www.freshbusinessthinking.com/business_advice.php?CID=3&AID=2629&PGID3 (date of access: 16.09.2022).
3. Tawileh A., Hilton J., McIntosh S. Managing information security in small and medium sized enterprises: a holistic approach. *ISSE/SECURE 2007 securing electronic business processes*. Wiesbaden. P. 331–339. URL: https://doi.org/10.1007/978-3-8348-9418-2_35 (date of access: 16.09.2022).
4. Park J.Y., Robles R.J., Hong C.H., Yeo S.S., Kim T. IT Security Strategies for SME's, International Journal of Software Engineering and its Applications. 2008. 2(3), July. P. 91-98

5. McNally W., Tenner A. R., DeToro I. J. Total quality management. three steps to continuous improvement. *The journal of the operational research society*. 1993. Vol. 44, no. 1. P. 91. doi: https://doi.org/10.2307/2584442 (date of access: 16.09.2026).
6. Volot O. I. Informatsiina ta kibernetychna bezpeka suchasnoho pidpryiemstva: zabezpechennia ta modeliuvannia. Tsentralnoukrainskyi naukovyi visnyk. Ekonomichni nauky. 2019. 3 (36). S. 238–247.
7. Donets L., Vashchenko N. Ekonomichna bezpeka pidpryiemstva: navch. posib. Kyiv: Tsentr uchb. lit., 2008. 240 s.
8. Perehiniak N., Diuk O. Osoblyvosti diialnosti suchasnoho menedzhera bezpeky. Formuvannia stratehii sotsialno-ekonomichnoho rozvytku pidpryiemnytskykh struktur v Ukraini: materialy Vseukr. naukovo-prakt. internet-konf., m. Lviv, 19–21 lystop. 2015 r. Lviv, 2015. S. 168.
9. Bakai V. Y., Zyma V. M. Novi vyklyky ta osoblyvosti stvorennia systemy informatsiinoi bezpeky pidpryiemstva. Visnyk Khmelnytskoho natsionalnoho universytetu. Ekonomichni nauky. 2020. № 5. S. 19–22.
10. Standart informatsiinoi bezpeky ISO / IEC 27002. URL: https://uk.wikipedia.org/wiki/ISO/IEC_27002 (data zvernennia: 10.09.2022 r.).