***Наумова Т. А.**, к.е.н., доцент,*
Державний біотехнологічний університет
***Акімова Н. С.**, к.е.н, професор,*
Державний біотехнологічний університет

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВЛАСНОЇ ІНФОРМАЦІЇ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ

Інформаційне суспільство являє собою сучасну систему даних з високим рівнем розвитку інформаційної культури, яке характеризується здатністю якісно продукувати всю необхідну для життєдіяльності суспільства інформацію, наявністю розвиненої інформаційної інфраструктури, високим рівнем доступності всіх громадян до необхідних даних та великою часткою працездатного населення, що трудиться в інформаційному секторі економіки. В умовах цифрової трансформації економіки, з урахуванням побудови інформаційного суспільства, все більшої актуальності набувають питання організаційного забезпечення захисту власної інформації підприємства. Отже, актуальним напрямом досліджень є проблема інформаційної безпеки підприємства в умовах цифрової трансформації економіки.

Вирішенню проблем захисту інформації присвячено праці багатьох науковців: Н.С. Акімова, Т.А. Наумова, Т.В. Петреман, О.В. Топоркова., К. О. Утенкова, В.В. Халецька. Вагомий внесок у розвиток теоретичних основ та проблематики інформаційної безпеки також зробили: Г. М. Азаренкова, Л. А. Бехтер, О. В. Дейнега, Т.Жук, В. Кузьомко, О.А., Панченко, Л.В. Панченко, Т.Ю. Ткачук, К. Фокіна-Мезенцева, В. Чубаєвський.

Метою дослідження є визначення організаційних проблем, що стосуються формування ефективної системи захисту інформації на підприємстві.

Обравши євроінтеграційний курс та визначивши вступ до НАТО своїм стратегічним пріоритетом, Україна має орієнтуватися передусім на стратегію розвитку країн-учасниць ЄС та НАТО в інформаційній сфері. Для нашої держави імплементація європейських стандартів правового забезпечення інформаційної безпеки держави є пріоритетним засобом інтеграції в європейський правовий простір [1, с. 30]. Внаслідок унікального геополітичного розташування, багатства духовної та історичної спадщини українського народу, Україна має стати інформаційно розвиненою державою, повноправним і впливовим учасником європейського життя, посісти гідне місце у глобалізованому світі, забезпечивши при цьому захист власного інформаційного простору від небажаного інформаційного впливу. Розвиток України можливий тільки за умов забезпечення належного рівня її інформаційної безпеки.

Під впливом COVID-19 активно розвивалася онлайн-сфера бізнесу. Торговельні підприємства не стали винятком, у зв’язку з чим підвищився рівень кіберзагроз. Кіберзагрози

для підприємств торгівлі пов'язані з шифруванням або викраденням даних клієнтів, уповільненням торговельних процесів. Це, в свою чергу, призводить до значних витрат підприємства. Натомість за умови успішної кібератаки вартість цифрової безпеки підприємств торгівлі суттєво збільшиться, а втрати включатимуть не тільки оголошений викуп за викрадену або зашифровану інформацію [2, с. 111].

В. Кузьомко, досліджуючи питання актуальних загроз інформаційній безпеці бізнесу, які формуються в умовах цифрової трансформації економіки, визначив, що проблема інформаційної безпеки бізнесу в умовах цифровізації економіки набуває особливої актуальності, а ті загрози, які породжує цифрова трансформація можуть бути успішно подолані лише взаємопов'язаною дією технічних, організаційних та економічних методів та засобів. Відповідно одним з пріоритетних напрямів забезпечення інформаційної безпеки бізнесу має стати постійне підвищення рівня інформаційної (цифрової) грамотності працівників та усебічне організаційно-документальне врегулювання процесів збору, накопичення, обробки використання і зберігання інформації в системі положень і інструкцій поводження з інформацією, які можуть імплементуватися в їх посадові інструкції. Такі завдання відповідають організаційному напряму забезпечення інформаційної безпеки бізнесу, який додатково охоплює такі дії, як визначення відповідальних за дотримання тих або інших заходів інформаційної безпеки, формування спеціалізованих на інформаційному захисті підрозділів в рамках організаційної структури організації, імплементацію положень нормативно-правових актів держави щодо кібербезпеки та захисту інформації в діяльність суб'єктів бізнесу тощо [3, с. 28].

О.В. Дейнега також вважає, що для забезпечення захисту інформації підприємство може застосовувати організаційний, технічний методи та здійснювати правове забезпечення захисту власної інформації [4, с. 77]. Автор відзначає, що формування системи захисту інформації повинно насамперед здійснюватися за принципом економічної доцільності, адже як халатне ставлення до зберігання (захисту) інформації, так і надмірне її засекречування однаковою мірою можуть викликати втрату частини прибутку чи призвести до непоправних економічних втрат. Як показує українська практика, на більшості підприємств і досі не сформована «культура захисту інформації», тобто до виникнення критичної ситуації, що спричинена витоком важливої конфіденційної інформації, підприємець або відповідальний менеджер вважає, що діяльність його організаційної структури нікого не цікавить або що шпигунство – це явище несправжнє, суто літературне. Слід зазначити, що в умовах, коли на ринку при сутній більше, ніж один виробник (продавець) певного товару, між ними найчастіше виникає конкурентна боротьба, яка в умовах нерозвитого ринку нерідко є недобросовісною, а одним із методів недобросовісної конкуренції є, як відомо, промислове шпигунство, поява якого обумовлена розвитком ринкової системи господарювання, розпадом

системи жорсткого контролю за виробництвом спеціальної техніки та ввезенням її в країну по офіційних і неофіційних каналах [4, с. 74].

Ми вважаємо, що саме організаційне забезпечення захисту власної інформації підприємства в умовах цифрової трансформації економіки є актуальним та першочерговим завданням. На жаль, керівники підприємств електронної комерції в належному ступені усвідомлюють серйозність інформаційних загроз і важливість організації захисту своїх ресурсів тільки після того, як останні піддатися інформаційним атакам.

На думку багатьох науковців, важливою складовою показної сторони інформації є інформаційне середовище, що має, у свою чергу, дві складові: організаційну і технологічну. Організаційна складова включає виробництво засобів інформатизації і інформаційних послуг, інформаційний ринок, підготовку і перепідготовку кадрів, проведення наукових досліджень. Визначають культуру інформаційної безпеки «як спосіб організації і розвитку інформаційного суспільства, що забезпечує якісне інформаційне середовище (якість споживаної інформації, захищеність суб'єкта від негативних інформаційних дій), створює можливість повністю задовольнити інформаційні потреби суб'єкта, і при якому він усвідомлює себе суб'єктом інформаційної безпеки, здатний виявити загрози, володіє технологіями захисту від них, дотримується норм інформаційної етики в процесі перетворення інформаційного середовища. Вона формується протягом всього життя людини в процесі безперервного навчання, виховання і самовиховання, чому сприяє високий рівень інформаційної культура та грамотності суспільства» [5, с. 37].

Таким чином, підсумовуючи різні погляди та визначення відомих науковців, ми вважаємо, що Інформаційна безпека, це процес створення відповідних умов щодо формування ефективної системи захисту та обміну інформацією на підприємстві. Відповідно, Інформаційна культура - організаційний процес, що забезпечує захищеність інформаційного середовища підприємства, у ході якого якісно та своєчасно виявляються та попереджаються негативні інформаційні дії, який супроводжується дотриманням етичних норм, правил та стандартів.

Ми підтримуємо позицію багатьох науковців, що для забезпечення захисту інформації підприємство може застосовувати організаційний, технічний методи та здійснювати правове забезпечення захисту власної інформації. Враховуючи ці пропозиції, нами були розширені напрямки захисту інформації та визначене місце організаційного методу в структурній композиції інформаційної безпеки підприємства (рис.1).

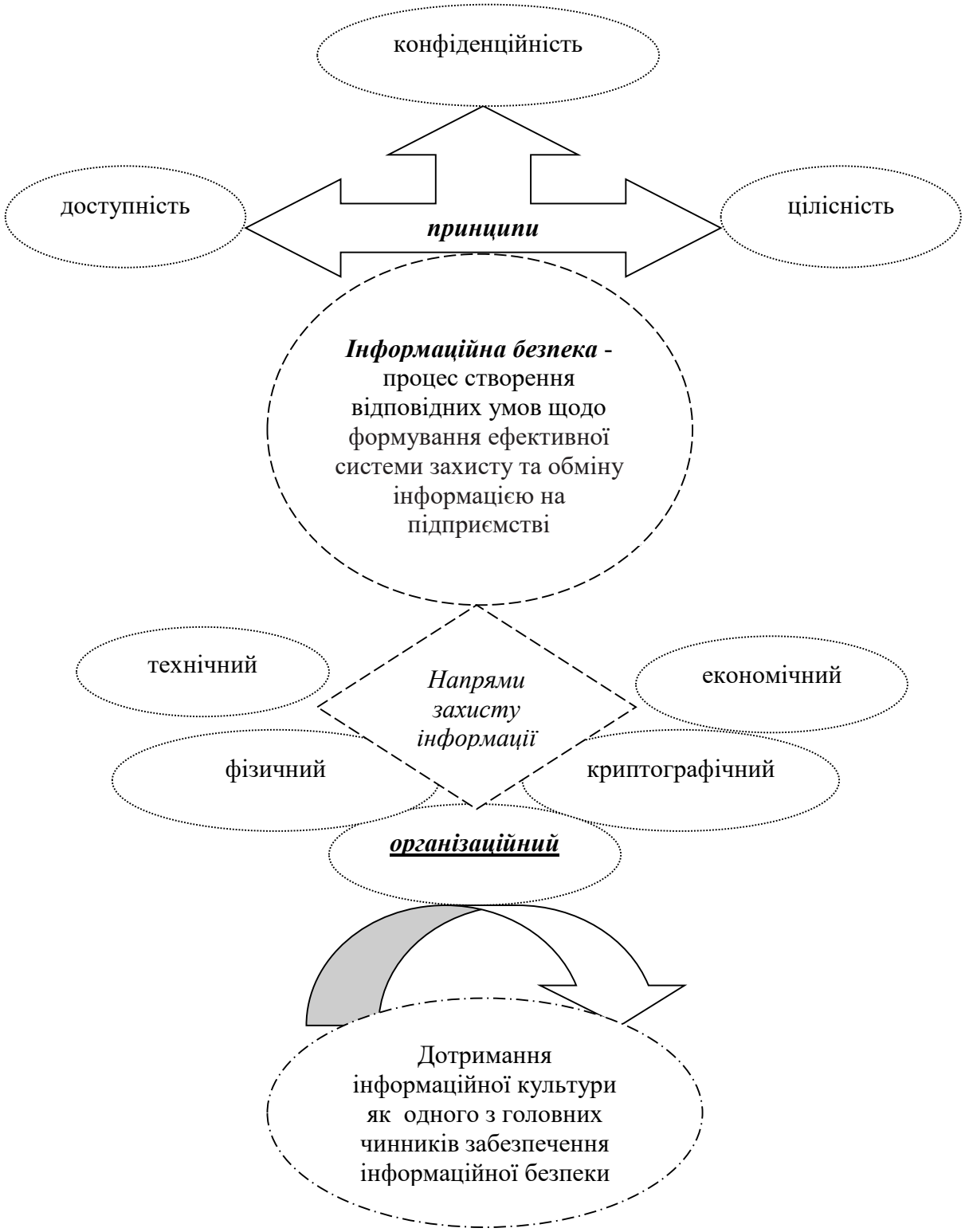

Рис. 1 – Місце організаційного напрямку захисту інформації в структурній композиції інформаційної безпеки підприємства

У цьому контексті нашого дослідження ми дійшли висновку, що серед основних вимог до проведення комерційних операцій підприємствами е-бізнесу є конфіденційність, цілісність, аутентифікація, авторизація, гарантії і збереження таємниці. При досягненні безпеки

інформації забезпечення її доступності, конфіденційності, цілісності та юридичної значимості є базовими завданнями.

Кожна загроза повинна розглядатися з точки зору того, як вона може торкнутися ці чотири властивості або якості безпечної інформації. Конфіденційність означає, що інформація обмеженого доступу повинна бути доступна тільки тому, кому вона призначена. Під цілісністю інформації розуміється її властивість існування в неспотвореному вигляді. Доступність інформації визначається здатністю системи забезпечувати своєчасний безперешкодний доступ до інформації суб'єктів, що мають на це належні повноваження. Юридична значимість інформації набуває важливість останнім часом, разом із створенням нормативно-правової бази безпеки інформації в нашій країні. Якщо перші чотири вимоги можна забезпечити технічними засобами, то виконання двох останніх залежить і від технічних засобів, і від організаційних, тобто відповідальності окремих осіб і організацій, а також від дотримання законів, що захищають споживача від можливого шахрайства продавців. Залишається ще низка питань, дослідження яких спрямоване на розроблення концептуальних правових засад забезпечення інформаційної безпеки держави та практичних рекомендацій щодо вдосконалення механізмів її реалізації в Україні.

Список використаних джерел:

1. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України. Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 — адміністративне право і процес; фінансове право; інформаційне право (081 — Право). – ДВНЗ «Ужгородський національний університет». 2019. С. 487. URL: URL: https://www. uzhnu. edu. ua/uk/infocentre/get/19617

2. Чубаєвський В., Жук Т. Економічна ефективність інформаційної безпеки підприємств торгівлі. Цифрова економіка. 2022. №1. С. 106-117. URL: http://doi.org/10.31617/visnik.knute.2022(141)08

3. Кузьомко В. Інформаційна безпека бізнесу в умовах цифрової трансформації економіки : зб. наук. пр. ДВНЗ «КНЕУ ім. Вадима Гетьмана». 2021. С. 26-28. URL: https://ir.kneu.edu.ua/handle/2010/36159

4. Дейнега О.В. Інформаційна безпека підприємств в умовах глобалізації 4.0. Економіка та суспільство.2019. Вип.20. С.70-79. URL: DOI: https://doi.org/10.32782/2524-0072/2019-20-28

5. Панченко О.А., Панченко Л.В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. “Правова інформатика”. 2015. № 2(46). С.32-38. URL: http://ippi.org.ua/panchenko-oa-panchenko-lv-informatsiina-bezpeka-ta-informatsiina-kultura-v-suchasnomu-informatsiinom