# ЗАГАЛЬНІ ПИТАННЯ

УДК 316.334.23:[004.056.5]

к.е.н., доц. **Городянська Л.В.** (ВІКНУ)
**Цюкало Л.В.** (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2021/70-11

## ІНФОРМАЦІЙНА БЕЗПЕКА СУБ'ЄКТІВ МАЛОГО ПІДПРИЄМНИЦТВА В УМОВАХ ЦИФРОВІЗАЦІЇ

***У статті визначено й проаналізовано характерні ознаки цифровізації сучасного суспільства, зокрема цифрової економіки. Зазначено, що прогрес у середовищі цифрових технологій вимагає застосування заходів інформаційної безпеки, в першу чергу, в фінансово-економічній діяльності суб'єктів малого підприємництва. Уточнено тлумачення дефініцій «інформаційна безпека» та «економічна безпека». Звертається увага на свідоме розуміння взаємодії між людьми й технологіями під час цифрової трансформації економіки таким чином, що новітні технології повинні адаптуватися до людей, а не навпаки. Підкреслюється, що таке розуміння може прийти лише в процесі навчання й набуття відповідних фахових компетентностей, особливо в середовищі суб'єктів малого підприємництва. Визначено види інформації суб'єктів малого підприємництва, які підлягають захисту, та складові економічної безпеки. Сформовано пропозиції щодо створення комплексної програми безпеки, до складу якої мають увійти план дій, спрямований на захист від зовнішнього та внутрішнього впливу на функціонування інформаційної системи підприємства, і комплекс заходів, призначений для захисту конфіденційності, доступності, цілісності даних від внутрішніх і зовнішніх, шкідливих та випадкових загроз. Інформаційна безпека суб'єктів малого підприємництва в умовах цифровізації має базуватися на таких позиціях: керівництво підприємства повинно регулярно проводити навчання всіх співробітників принципам інформаційної безпеки, захисту даних та убезпечити фізичні носії даних від кібератак; корпоративна мережа має бути сегментована, а доступ до неї – контрольованим; партнерська співпраця з постачальниками послуг з позицій інформаційної безпеки має бути рівнозначною; віддалений доступ до корпоративної мережі підприємства має бути максимально захищеним і відповідати нормам інформаційної безпеки. Вважається, що найбільш дієвими напрямами підвищення інформаційної безпеки суб'єктів малого підприємництва на державному рівні в умовах цифровізації суспільства є впорядкування спрощеної системи оподаткування, сприяння розвитку інноваційного підприємництва, формування сучасної інформаційної інфраструктури підтримки підприємництва тощо.***

***Ключові слова: цифровізація, цифрова технологія, цифрова економіка, суб'єкт малого підприємництва, інформаційна безпека, економічна безпека, захист інформації.***

**Вступ та постановка проблеми.** Характерною ознакою сучасного глобалізованого світу є насичення усіх видів діяльності електронно-цифровими пристроями та засобами, системами й технологіями налагодження електронного комунікаційного обміну між ними. Це соціальне явище отримало назву – цифровізація або цифрові технології. На жаль, всі ці новітні й перспективні технології, застосовувані в суспільному житті й економіці, стають дуже привабливими для кіберзлочинців по всьому світу і вимагають певних заходів інформаційної безпеки, в першу чергу, в царині суб'єктів малого підприємництва (СМП), які в сучасних умовах відіграють провідну роль в суспільстві й державі.

Загрози в інформаційному світі можуть виникнути в будь-який момент «спілкування» з Інтернетом, де кіберзлочинці можуть скористатись доступом до конфіденційної інформації через фішинг-повідомлення електронної пошти, підробку в мережах, або через пошкоджене обладнання. Ризик наразитися на кіберзагрозу, пов'язану з витоком комерційної або конфіденційної інформації підприємства, суттєво зростає зі збільшенням кількості пристроїв в мережі, а також з поширенням в бізнесі хмарних обчислень. Саме тому стає життєво важливою проблема необхідного забезпечення інформаційної безпеки на підприємствах, що

передбачає розробки й застосування певних заходів і дотримання відповідних правил і вимог для безпечного та безперервного функціонування підприємства в умовах цифрової економіки.

**Аналіз останніх досліджень і публікацій.** Проблемам дослідження економічної безпеки суб'єктів підприємницької діяльності, банків та інших організацій, а також основним тенденціям їх розвитку в сучасних умовах цифровізації суспільства присвячено праці багатьох авторів і чинні нормативні акти державних органів [1-18].

Вперше визначення «економічна безпека» з'являється приблизно в період соціально-економічних реформ у США, що супроводжувались економічним спадом в країні. Франклін Рузвельт [10, с. 37] розглядав економічну безпеку в контексті національної безпеки країни. Коли в 1985 р на 40-й сесії Генеральної Асамблеї ООН було прийнято резолюцію щодо міжнародної економічної безпеки, категорія «економічна безпека» набула офіційного статусу.

Огляд аналітичних доповідей і чинних документів [1-3; 5-9] разом із науковими працями [4; 11-18] показав всеосяжний характер вирішення проблеми економічної та інформаційної безпеки та її актуалізацію на різних рівнях економіки від мікро- до макрорівня. Дотримання вимог економічної безпеки є актуальною, дефініція «економічна безпека» в літературі [1-18] пов'язана з державною економічною політикою, економічною незалежністю, стабільністю національної економіки, інформаційною безпекою, безпекою банківської системи, здатністю підприємства до економічного розвитку та залежить від зміни умов зовнішнього середовища. Зазвичай фінансова та господарська діяльність суб'єктів малого підприємництва в сучасних умовах господарювання нерозривно пов'язана з використанням цифрових технологій. Інтеграція цифрових технологій із фінансовою сферою призвела до появи нових віртуальних форм банків, які стають все більш популярними серед користувачів та, безумовно, серед суб'єктів підприємницької діяльності. Суб'єкт підприємницької діяльності обов'язково використовує мережу Internet та банкінг для здійснення банківських операцій, наприклад, задля сплати податків, платежів, розрахунків з постачальниками та замовниками робіт (послуг) та інших фінансових операцій. Банківська сфера діяльності активно розвивається та є досить привабливим об'єктом інтересу кіберзлочинчів [4]. Слушною є думка вчених С.В. Ленков, Д.А. Перегудов, В.А. Хорошко, які зазначають, що доступ до інформаційних ресурсів може бути обмежений задля досягнення інформаційної безпеки суб'єктів підприємництва [14].

Дефініції «економічна безпека» та «інформаційна безпека» на мікрорівні досліджували такі вчені як Т.Г. Васильців, В.І. Волошин, О.Р. Бойкевич, В. В. Каркавчук [11], С.М. Ілляшенко [12], Д. Ковалев, Т. Сухорукова [13], С.В. Ленков, Д.А. Перегудов, В.А. Хорошко [14]; О.Ф. Новікова, Р.В. Покотиленко [15], І.А. Федоренко [16], А. Яніогло [17] та інші. Зокрема, вчені Д. Ковальов та Т. Сухорукова [13] тлумачили дефініцію «економічна безпека» в контексті захисту підприємства від впливу загроз. Автори вважали, що економічна безпека має сприяти захисту підприємства від впливу існуючих факторів зовнішнього та внутрішнього середовища та підкреслювати потребу в уникненні негативних наслідків та можливих загроз у процесі діяльності. На думку А. Яніогло [17] «економічна безпека» є станом, що характеризує здатність суб'єкта підприємництва забезпечити ефективне використання підприємницьких можливостей та ресурсів з метою уникнення загроз та досягнення мети діяльності. Вважаємо, що дефініцію «економічна безпека» на мікрорівні доцільно дослідити з позиції підприємства як економічної системи, що знаходиться у динамічному розвитку. Складовими взаємопов'язаними елементами такої системи є фінансові ресурси, економічні ресурси та трудові ресурси суб'єкта малого підприємництва. Створення умов стабільного розвитку системи та її елементів, виявлення та попередження зовнішніх та внутрішніх загроз є важливими завданнями економічної й, особливо, інформаційної безпеки підприємства.

В контексті усього вище наведеного вирішення потребує низка питань, зокрема тих, що відносяться до інформаційної безпеки суб'єктів малого підприємництва. Слід зазначити, що цифрова економіка за визначенням містить нові можливості й для людини, і для суспільства, оскільки людина завжди бере участь у процесі виробництва товарів (робіт, послуг), є суб'єктом діяльності і має бути в центрі процесу діяльності. Цифрова трансформація

економіки вимагає свідомого розуміння взаємодії між людьми й технологіями, і ті, хто розуміє, що технології повинні адаптуватися до людей, а не навпаки, мають шанси на успіх. Таке розуміння може прийти лише в процесі навчання й набуття відповідних фахових компетентностей. Статус особистості дедалі більше залежить від освіти та активної життєвої позиції, як підкреслено у [1]. На жаль, зараз спостерігається неналежна якість професійно-технічної та вищої освіти, що зазначено в [2, с. 27]. Все це призводить до нових або зміни існуючих видів діяльності. Внаслідок стрімкого розвитку інформаційного світу й глобалізації суспільства відбувається зміна пріоритетів професійно-трудової діяльності людини, яка відтепер пов'язана з розвитком та перенесенням акцентів з матеріальних засобів праці на нематеріальні, цифрові, персональні обчислення. Що й породило додаткові ризики й загрози для безпеки як у повсякденному житті суспільства, так і для фінансово-господарської діяльності суб'єктів підприємництва.

**Метою статті** є формування пропозицій щодо напрямів інформаційної безпеки суб'єктів малого підприємництва в умовах цифровізації.

Досягнення мети передбачає виконання таких завдань:

- уточнити сутність понять «економічна безпека» та «інформаційна безпека»;
- визначити види інформації суб'єктів малого підприємництва, які потребують захисту;
- надати пропозиції щодо напрямів інформаційної безпеки суб'єктів малого підприємництва в умовах цифровізації.

**Виклад основного матеріалу дослідження.** У сучасних умовах загального економічного спаду та недостатньої державної економічної політики суб'єкти малого підприємництва повинні створювати умови для протидії внутрішнім та зовнішнім загрозам і ризикам, визначаючи пріоритетні напрями посилення своєї економічної безпеки. Огляд чинної нормативної та наукової літератури [1-17] надав можливість дослідити сутність «економічної безпеки» та сформулювати узагальнене визначення цієї дефініції. Отже, економічна безпека є комплексом дієвих заходів офіційних державних органів, які забезпечують стійкість до зовнішніх і внутрішніх загроз, який характеризує здатність національної економіки до розширеного самовідтворення та задоволення потреб громадян, суб'єктів підприємництва, суспільства і держави на певному визначеному рівні та часовому проміжку.

Використання інформаційних технологій, наприклад, таких як технологія великих даних, штучний інтелект, технологія блокчейн, квантові технології, робототехніка, віртуальна реальність тощо, потребують визначення функціональних складових економічної безпеки суб'єктів підприємства. На основі комплексного аналізу нормативної, зарубіжної та вітчизняної літератури [7; 11-16; 17, с. 21] було визначено основні функціональні складові економічної безпеки СМП на мікрорівні (рис. 1).

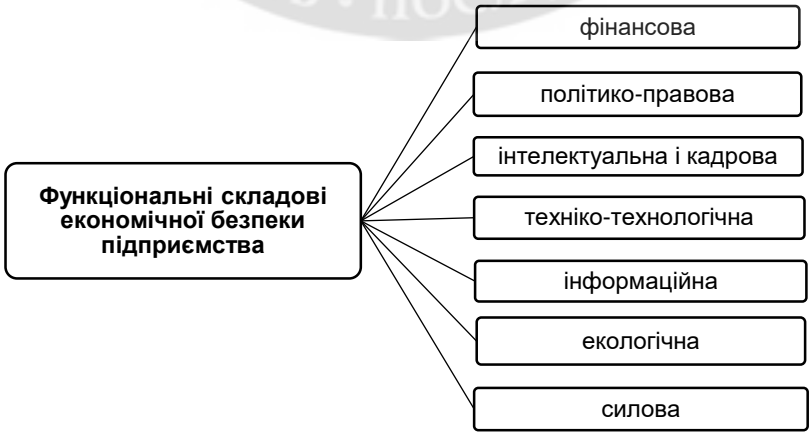


Рисунок 1 – Функціональні складові економічної безпеки СМП на мікрорівні (розробка авторів на базі джерел [7; 11-16; 17, с. 21])

Охарактеризуємо сутність кожної функціональної складової економічної безпеки суб'єктів підприємництва:

- фінансова складова характеризує досягнення суб'єктом підприємництва раціонального використання ресурсів;
- політико-правова складова характеризує дотримання суб'єктом підприємництва вимог чинного законодавства, всебічне правове забезпечення правової діяльності підприємства;
- інтелектуальна і кадрова складові відображають рівень збереження і розвиток інтелектуального потенціалу, ефективне управління суб'єктами підприємництва відтворенням потенціалу персоналу;
- техніко-технологічна складова характеризує ступінь відповідності технологій, які застосовуються суб'єктами підприємництва, сучасним світовим аналогам за умови оптимізації витрат ресурсів;
- інформаційна складова характеризує ефективне інформаційно-аналітичне забезпечення суб'єктами підприємництва власної фінансово-господарської діяльності;
- екологічна складова характеризує дотримання суб'єктами підприємництва чинних екологічних норм;
- силова складова характеризує забезпечення суб'єктами підприємництва фізичної безпеки працівників.

Проблема формування комплексних знань, навичок і умінь працівника, які є необхідними для підтримки цілей безпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту є актуальною як на макро-, так і на мікрорівні. Пропозиції щодо напрямів відтворення інтелектуального потенціалу в умовах цифрових технологій розкрито у праці [18, с. 96-99]. Відтворення інтелектуального потенціалу персоналу, що є неідентифікованим ресурсом підприємства, доцільно планувати, спираючись на механізм відтворення інтелектуальних ресурсів підприємств та алгоритм прогнозного аналізу відтворюваних економічних ресурсів [18, с. 98; 19, с. 42-44; с. 225-228].

Визначимо особливості класифікації (типологію) підприємств України (табл. 1) з врахуванням нових змін до Закону України «Про бухгалтерський облік та фінансову звітність в Україні» [20]. Ці зміни були внесені у зв'язку з потребою в адаптації законодавства відповідно до вимог МСФО та Директиви 2013/34/ЕС Європейського парламенту та Ради від 26.06.2013 року. Уточнимо критерії віднесення підприємств до СМП згідно вимог чинного законодавства [3; 6; 8; 20].

Відповідно до вимог [3; 6, с. 17; 20] підприємства (крім бюджетних установ) можуть належати до суб'єктів малого підприємництва, середнього або великого (табл. 1).

Таблиця 1

Класифікація суб'єктів підприємництва за розміром бізнесу
(складено авторами згідно з даними [3; 6, с. 17; 20])

| Ознака суб'єктів підприємництва | Суб'єкти малого підприємництва | | Суб'єкти середнього підприємництва | Суб'єкти великого підприємництва |
|---|---|---|---|---|
| | Мікро підприємства | Малі підприємства | | |
| Балансова вартість активів | До 350 тис. € | До 4 млн. € | До 20 млн. € | Понад 20 млн. € |
| Чистий дохід | До 700 тис. € | До 8 млн. € | До 40 млн. € | Понад 40 млн. € |
| Середня чисельність працюючих | До 10 чоловік | До 50 чоловік | До 250 чоловік включно | Понад 250 чоловік |

У дослідженні згідно з [3] мікропідприємства та малі підприємства вважаються суб'єктами малого підприємництва. Відповідно до статті 2 Закону [20] визначені критерії віднесення підприємств до суб'єктів малого підприємництва, це зокрема: балансова вартість активів; чистий дохід від реалізації продукції (товарів, робіт, послуг); середня кількість працівників. Аналіз таблиці 1 показав, що чисельність працівників різних за розміром бізнесу видів підприємств може варіюватися від 10 до понад 250 чоловік. Навчання трудових ресурсів доцільно організувати на усіх без винятку підприємствах. Зазвичай керівник малого підприємства (до 10 чол.) за браком часу та обмеженої кількості трудових ресурсів уникає забезпечення вимог інформаційної безпеки. Однак йому варто володіти знаннями про можливі ризики. Варто також враховувати й морально-психологічні наслідки недотримання вимог інформаційної безпеки для користувачів, персоналу і власників бізнесу.

Згідно зі ст. 13 Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [7] «інформаційна безпека» тлумачиться як «стан захищеності життєво важливих інтересів людини, суспільства й держави, при якому запобігається нанесення шкоди» через:

–неповноту, невчасність та невірогідність інформації, що використовується;

–негативний інформаційний вплив;

–негативні наслідки застосування інформаційних технологій;

–несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Суб'єкти малого підприємництва [3] володіють цінною інформацією (наприклад, конфіденційною інформацію про бізнес, про ділові якості працівників та персональну інформацію щодо клієнтської бази та ін.). Досить важливою для суб'єктів малого підприємництва є інформація про фінансовий стан, конкурентоспроможність продукції, кількісний і якісний склад персоналу. Керівництво має ухвалювати рішення про те, хто і як визначатиме ступінь конфіденційності і важливості інформації. Відповідно до ст. 20 Закону України «Про внесення змін до Закону України «Про інформацію» [21] інформація, за порядком доступу поділяється «на відкриту інформацію та інформацію з обмеженим доступом». В контексті інформаційного забезпечення підприємства різними видами інформації, яка призначена для ухвалення господарських управлінських рішень, зазвичай вживаються різні критерії класифікації інформації. Наприклад, у фінансовому розрізі використовується передусім економічна інформація, яка за функціональним призначенням поділяється на нормативну, планову, облікову, аналітичну та прогнозну інформацію. Економічна інформація структурується відповідно до поставлених цілей і завдань впливу на об'єкт управління та є різновидом управлінської інформації. Інформація є важливим елементом системи управління підприємством, тому що володіння, повною, достовірною, актуальною та оперативною інформацією забезпечує можливість прийняття ефективних управлінських рішень. Розрізняють такі види інформації:

–*вхідна* (внутрішня) інформація, яку отримають в результаті відображення та фіксації тим чи іншим способом змін у господарських явищах і процесах;

–*вихідна* (зовнішня) інформація, яка накопичується в результаті обробки даних.

Для суб'єктів малого підприємництва з огляду на захист інформаційних ресурсів важливою є вихідна інформація. Вихідну інформацію для підприємств поділяють на:

–інформацію про стан зовнішнього середовища, яка містить дані про ринкову кон'юнктуру;

–інформацію про передумови створення та фінансовий стан підприємства.

Вважаємо, що сутність інформаційної складової безпеки підприємства полягає у формуванні принципів, методів і заходів щодо виявлення, аналізу, запобігання та нейтралізації негативних джерел, причин і умов впливу на інформацію щодо господарської діяльності підприємства. При цьому поняття «інформаційна безпека» характеризує стан інформаційного захисту господарюючого суб'єкта в умовах, коли існує ймовірність загроз, що досягається

системою заходів, спрямованих на попередження, виявлення та ліквідацію інформаційних загроз. Можливість реалізації загроз залежить від наявності вразливих місць в інформаційній системі. Склад і специфіка вразливих місць визначається:

−типом вирішуваних завдань;

−характером інформації;

−апаратно-програмними особливостями обробки інформації на підприємстві;

−наявністю засобів захисту та їхніми характеристиками.

З позиції інформаційних технологій захисту інформації інформаційна безпека – це система заходів, що дає змогу виявляти: вразливі місця інформаційно-комунікаційної системи підприємства; небезпеки, які загрожують їй, і методи нейтралізації виявлених загроз. Під загрозою треба розуміти подію, яка може викликати порушення функціонування інформаційної системи, включаючи спотворення, знищення або несанкціоноване використання бази даних підприємства.

Таким чином, спектр інтересів інформаційної безпеки щодо інформації, інформаційних систем та інформаційних технологій як об'єктів безпеки можна поділити на такі основні категорії:

1) доступність – можливість за визначений час отримати певну інформаційну послугу;

2) цілісність – релевантність та несуперечливість інформації, її захищеність від руйнування та несанкціонованого змінювання;

3) конфіденційність – захищеність від несанкціонованого доступу.

Інформація на підприємстві є важливим комерційним активом. Це вимагає створення відповідної системи її захисту, що важливо в умовах бізнесу, де інформація наражається на все більшу кількість та різноманітність загроз і вразливих місць. Нанесення таких видів збитків, як зловмисний код, «злом» комп'ютера та інші кібератаки, стають все більш поширеними, амбітними та складнішими. Дотримання вимог інформаційної безпеки на підприємстві в умовах цифровізації передбачає планування заходів з регулярного навчання всіх співробітників, які працюють з даними, з метою уникнення людських за характером загроз і збереження інформації.

Однією із цілей інформаційної безпеки є захист даних, які підприємство збирає та використовує. Якщо інформація залишається незахищеною, до неї може отримати доступ будь-хто. Якщо інформація потрапить в чужі руки, вона може зруйнувати життя, бізнес, а також може бути використана для заподіяння шкоди. Сутність безпеки пов'язана з якістю або станом безпеки в контексті уникнення шкоди. Науковці С.В. Ленков, Д.А. Перегудов, В.А. Хорошко [14] підкреслюють, що метою інформаційної безпеки є захист інформації та її критичних елементів разом із системами та обладнанням, за допомогою яких використовують, зберігають та передають інформацію. Тобто це сукупність технологій, стандартів, політики та практик управління, які застосовують до інформації з метою її збереження. Враховуючи слушну думку вітчизняних вчених С.В. Ленков, Д.А. Перегудов, В.А. Хорошко [14] та зарубіжних авторів Вітмен і Маттор [22], запропоновано класифікацію (рис. 2), де визначено важливі функції інформаційної безпеки для суб'єктів підприємництва.

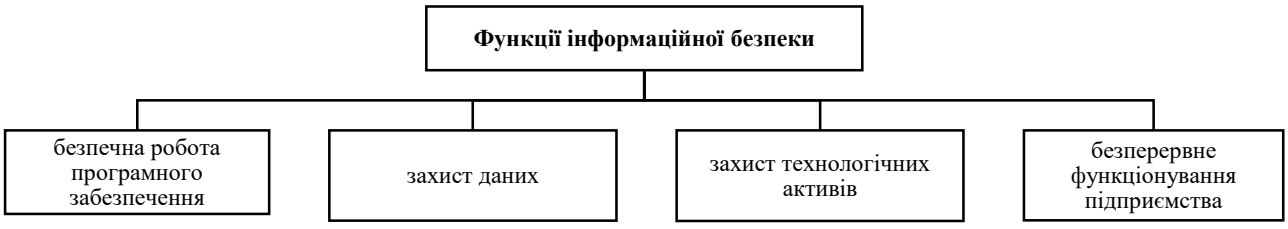


Рисунок 2 – Функції інформаційної безпеки підприємства
(розробка авторів на базі [14; 22])

Дотримання функцій інформаційної безпеки на підприємстві дозволить:

–забезпечувати безпечну роботу програмного забезпечення, що реалізовано в системах цифрових технологій будь-якого підприємства;

–здійснювати захист даних, які підприємство збирає та використовує;

–захистити технологічні активи, що використовуються на підприємстві;

–сприяти безперервному функціонуванню підприємства.

Програми інформаційної безпеки забезпечують захист відповідної інформації як за діловими, так і юридичними вимогами, вживши заходів щодо захисту даних підприємства. Крім того, такі заходи покликані забезпечити збереження конфіденційності, комерційних таємниць та запобігання крадіжці інформації.

Таким чином, впровадження засад забезпечення інформаційної безпеки на підприємстві дозволить захистити технологічні активи (нематеріальні активи), фінансові операції, комерційну та конфіденційну інформацію.

Виходячи із вище сказаного, можна сформулювати такі основні пропозиції щодо вибору й реалізації напрямів інформаційної безпеки суб'єктів малого підприємництва в умовах цифровізації:

1. Керівництво підприємства повинно мати комплексну програму безпеки та регулярно проводити навчання всіх співробітників, які працюють з даними, щодо принципів інформаційної безпеки та захисту даних, можливих способів атак зловмисників, а також методів їх уникнення.

2. Фізичні носії даних та робочі пристрої мають бути захищеними від кібератак та інфікування шкідливим програмним забезпеченням. Для цього потрібно завжди коректно виходити з систем та ресурсів, які містять конфіденційні дані, користуватися методами шифрування даних та здійснювати регулярне резервне копіювання файлів.

3. Корпоративна мережа має бути сегментована таким чином, щоб конфіденційні дані були розміщені на окремих ресурсах, а користувачі, які отримують або намагаються отримати доступ до мережі, підлягали детальному моніторингу. Це значно знизить навантаження на систему, забезпечить контроль доступу до мережі та її безпеку.

4. Партнерська співпраця з постачальниками послуг в сучасних спрощених умовах комунікацій має бути, з позицій інформаційної безпеки, рівнозначною. Тобто такою, коли рівень безпеки постачальника відповідає рівню безпеки замовника послуг.

5. Віддалений доступ до мережі підприємства, який зараз набуває все більшого поширення і вважається чи не єдиним способом розв'язання соціальних проблем, має бути максимально захищеним і відповідати нормам інформаційної безпеки.

**Висновки.** У статті досить детально розкриті поняття «економічна безпека» та «інформаційна безпека» стосовно суб'єктів підприємництва в умовах цифровізації суспільства. Розкрито типологію суб'єктів підприємництва в Україні, що побудована з врахуванням міжнародної практики.

Визначено основні види інформації суб'єктів малого підприємництва, які підлягають захисту, та способи забезпечення їх інформаційної безпеки. Запропоновано заходи щодо вибору й реалізації напрямів інформаційної безпеки суб'єктів малого підприємництва, які можуть бути покладені в основу розробки комплексної програми безпеки.

Перспективою подальших досліджень з врахуванням вимог оптимізації участі України в міжнародному поділі праці є розробка комплексу заходів на державному рівні, до якого відноситься впорядкування спрощеної системи оподаткування, сприяння розвитку інноваційного підприємництва, кластерна організація малого бізнесу, формування сучасної інформаційної інфраструктури підтримки підприємництва, формування сприятливого бізнес-клімату тощо.

ЛІТЕРАТУРА:

1.Про внутрішнє та зовнішнє становище України : Аналітична доповідь Національного інституту стратегічних досліджень до щорічного Послання Президента України до Верховної Ради України.

URL: https://niss.gov.ua/publikacii/poslannya-prezidenta-ukraini/analitichna-dopovid-do-schorichnogo-poslannya-prezidenta-4 (дата звернення: 24.02.2021).

2.Про Національну програму сприяння розвитку малого підприємництва в Україні : Закон України від 21 груд. 2000 року № 2157-III.URL: https://zakon.rada.gov.ua/laws/show/2157-14?find=1&text= (дата звернення: 24.02.2021).

3.Про затвердження Порядку надання фінансової державної підтримки суб'єктам мікропідприємництва та малого підприємництва : Постанова Кабінету Міністрів України від 24 січ. 2020 р. № 28. URL: https://zakon.rada.gov.ua/laws/show/28-2020-%D0%BF#n9 (дата звернення: 24.02.2021).

4.Gorodianska, L.V, Nosenko, T.I. & Vember, V.P. (2019) Neobanks operations and security features. Problems of Infocommunications. Science and Technology PIC S&T'2019: 2019 IEEE International Scientific and Practical Conference 08-11 October 2019 (pp. 839-842). – Kyiv. DOI: 10.1109/PICST47496.2019.9061268 [in Ukrainian].

5.Портал для підприємців // Міністерство розвитку економіки, торгівля та сільского господарства України : веб-сайт. URL: https://sme.gov.ua/analitychni-materialy (дата звернення: 24.02.2021).

6.OECD (2020), Моніторинг реалізації Стратегії розвитку МСП України на 2017-2020 роки // OECD Publishing, Paris. URL: https://sme.gov.ua/wp-content/uploads/2020/09/Monitoring_ the_Implementation_of_Ukraine-s_SME_Development_Strategy_uk.pdf (дата звернення: 23.02.2021).

7.Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09 січ. 2007 р. № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#n1 (дата звернення: 24.02.2021).

8.Що таке цифрова трансформація компанії? // Creatio – платформа для управління бізнес-процесами : веб-сайт. URL: https://www.terrasoft.ua/page/digital-transformation (дата звернення: 24.02.2021).

9.Україна 2030E – країна з розвинутою цифровою економікою // Український Інститут майбутнього. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html (дата звернення: 24.02.2021).

10.Франклин Р. Беседы у камина. О кризисе, олигархах и войне. Москва: Литагент Алгоритм, 2016. 408 с.

11.Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення : монографія / Васильців Т. Г., Волошин В. І., Бойкевич О. Р., Каркавчук В. В. / за ред. Т.Г. Васильціва. Львів : Ліга-Прес, 2012. 388 с.

12.Ильяшенко С.Н. Составляющие экономической безопасности предприятия и подходы к их оценке. *Актуальні проблеми економіки* : науковий журнал. 2003. № 3. С. 11-19.

13.Ковалев Д., Сухорукова Т. Экономическая безопасность предприятия. *Экономика Украины.* 1998. № 10. С. 48-51.

14.Ленков С. В., Перегудов Д. А., Хорошко В. А. Методы и средства защиты информации : монография в 2 т. / Киев : Арий, 2008. Т. 2 : Информационная безопасность / под ред. В. А. Хорошко. 343 с.

15.Новікова О.Ф., Покотиленко Р.В. Економічна безпека: концептуальне визначення та механізм забезпечення : монографія. Донецьк: Ін-т економіки промисловості НАН України, 2006. 408 с.

16.Федоренко І.А., Мейта В.І. Розвиток концептуальних підходів до визначення економічної безпеки промислових підприємств. *Інноваційна економіка.* 2013. № 5. С. 304-308 URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/ inek_2013_5_77.pdf (дата звернення 23.02.2021).

17.Яніогло А. Комплексная система обеспечения экономической безопасности предприятий (на примере АТО Гагаузия): дис. … д-ра екон.наук: 521.03. Кишинэу, 2017. 188 с.

18.Городянська Л.В. Напрями відтворення інтелектуального потенціалу підприємства в умовах цифрових технологій. *Нові інформаційні технології управління бізнесом* : збірник тез IV Всеукр. наук.-практ. конф., м. Київ, 11 лют. 2021 р.). Київ: Спілка автоматизаторів бізнесу, 2021. – С. 96-99.

19.Городянська Л. В. Відтворювані економічні ресурси: теорія та методологія обліку і аналізу : монографія. Київ: КНЕУ, 2013. 259 с.

20.Про бухгалтерський облік та фінансову звітність в Україні : Закон України від 16 липн. 1999 р. № 996-XIV. URL: https://zakon.rada.gov.ua/laws/show/996-14#Text (дата звернення: 24.02.2021).

21.Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12?find (дата звернення: 24.02.2021).

22.Global Cybersecurity Status Repor. (2015, January). ISACA International. Retrieved from https://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-StatusReport-Data-Sheet_ mkt_Eng_0115.pdf (дата звернення: 24.02.2021).

REFERENCES:

1. Pro vnutrishnje ta zovnishnje stanovyshhe Ukrajiny : Analitychna dopovidj Nacionaljnogho instytutu strateghichnykh doslidzhenj do shhorichnogho Poslannja Prezydenta Ukrajiny do Verkhovnoji Rady Ukrajiny (2020), niss.gov.ua/publikacii/poslannya-prezidenta-ukraini/analitichna-dopovid-do-schorichnogo-poslannya-prezidenta-4 (accessed 24 February 2021).

2. Pro Nacionaljnu proghramu spryjannja rozvytku malogho pidpryjemnyctva v Ukrajini : Zakon Ukrajiny (2000), zakon.rada.gov.ua/laws/show/2157-14?find=1&text= (accessed 24 February 2021).

3. Pro zatverdzhennja Porjadku nadannja finansovoji derzhavnoji pidtrymky sub'jektam mikropidpryjemnyctva ta malogho pidpryjemnyctva : Postanova Kabinetu Ministriv Ukrajiny (2020), zakon.rada.gov.ua/laws/show/28-2020-%D0%BF#n9 (accessed 24 February 2021).

4. Gorodianska, L.V, Nosenko, T.I. and Vember, V.P. (2019) «Neobanks operations and security features». *Problems of Infocommunications. Science and Technology (PIC S&T'2019: 2019 IEEE) International Scientific and Practical Conference*, Kyiv, 08-11 October 2019, pp. 839-842. DOI: 10.1109/PICST47496.2019.9061268.

5. Ministerstvo rozvytku ekonomiky, torghivlja ta siljskogho ghospodarstva Ukrajiny (2019). *Portal dlja pidpryjemciv*. [online] Available at: sme.gov.ua/analitychni-materialy (accessed 24 February 2021).

6. OECD Publishing, Paris (2020). *Monitoryngh realizaciji Strateghiji rozvytku MSP Ukrajiny na 2017-2020 roky*. [online] Available at: sme.gov.ua/wp-content/uploads/2020/09/Monitoring _the_Implementation_of_Ukraine-s_SME_Development_Strategy_uk.pdf (accessed 24 February 2021).

7. Pro Osnovni zasady rozvytku informacijnogho suspiljstva v Ukrajini na 2007-2015 roky : Zakon Ukrajiny (2007), zakon.rada.gov.ua/laws/show/537-16#n1 (accessed 24 February 2021).

8. Creatio platforma dlja upravlinnja biznes-procesamy (2020). *Shho take cyfrova transformacija kompaniji?* [online] Available at: www.terrasoft.ua/page/digital-transformation (accessed 24 February 2021).

9. Ukrajinsjkyj Instytut majbutnjogho (2020). *Ukrajina 2030E – krajina z rozvynutoju cyfrovoju ekonomikoju.* [online] Available at: strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html (accessed 24 February 2021).

10.Franklin, R. (2016), *«Besedyi u kamina. O krizise, oligarhah i voyne»* [Conversations by the fireplace. About the crisis, oligarchs and war], 408 p.

11.Vasyljciv, T.Gh. eds., Voloshyn, V.I., Bojkevych, O.R. and Karkavchuk, V.V. (2012) *«Finansovo-ekonomichna bezpeka pidpryjemstv Ukrajiny: strateghija ta mekhanizmy zabezpechennja: monoghrafija»* [Financial and economic security of Ukrainian enterprises: strategy and support mechanisms], Ljviv, 388 p.

12.Ilyashenko, S.N. (2003), «Sostavlyayuschie ekonomicheskoy bezopasnosti predpriyatiya i podhodyi k ih otsenke» [Components of economic security of the enterprise and approaches to their assessment], *AktualnI problemi ekonomiki*, № 3, pp. 11-19.

13.Kovalev, D. and Suhorukova, T. (1998), «Ekonomicheskaya bezopasnost predpriyatiya» [Economic security of the enterprise], *Ekonomika Ukrainyi*, № 10, pp. 48-51.

14.Lenkov, S.V., Peregudov, D.A., Horoshko, V.A. eds., (2008), *«Metodyi i sredstva zaschityi informatsii : monografiya., vol. Informatsionnaya bezopasnost»* [Methods and means of information protection, vol. 2: Information Security], Ariy, Kyiv, 343 p.

15.Novikova, O.F. and Pokotylenko, R.V. (2006) *«Ekonomichna bezpeka: konceptualjne vyznachennja ta mekhanizm zabezpechennja : monoghrafija»* [Economic security: conceptual design and mechanism of security], In-t ekonomiky promyslovosti NAN Ukrajiny, Donecjk, 408 p.

16.Fedorenko, I.A. and Mejta, V.I. (2013) «Rozvytok konceptualjnykh pidkhodiv do vyznachennja ekonomichnoji bezpeky promyslovykh pidpryjemstv» [Development of conceptual approaches to the value of economic security of industrial enterprises], *Innovacijna ekonomika*. № 5. pp. 304-308.

17.YanIoglo, A. (2017), *«Kompleksnaya sistema obespecheniya ekonomicheskoy bezopasnosti predpriyatiy (na primere ATO Gagauziya): dissertaion»* [Comprehensive system for ensuring the economic security of enterprises (on the example of ATU Gagauzia)], Kishineu,188 p.

18.Gorodianska, L.V. (2021) «Naprjamy vidtvorennja intelektualjnogho potencialu pidpryjemstva v umovakh cyfrovykh tekhnologhij» [Directions of reproduction of intellectual potential of the enterprise in the conditions of digital technologies]. *Novi informacijni tekhnologhiji upravlinnja biznesom* : zbirnyk tez IV Vseukr. nauk.-prakt. konf., Spilka avtomatyzatoriv biznesu, Kyiv, pp. 96-99.

19.Gorogianska, L. V. (2013) *«Vidtvorjuvani ekonomichni resursy: teorija ta metodologhija obliku i*

*analizu : monoghrafija»* [Recreating economic resources: theory and methodology of accounting and analysis], KNEU, Kyiv, 259 p.

20.Pro bukhghaltersjkyj oblik ta finansovu zvitnistj v Ukrajini : Zakon Ukrajiny (1999), zakon.rada.gov.ua/laws/show/996-14#Text (accessed 24 February 2021).

21.Pro informaciju: Zakon Ukrajiny (1992), zakon.rada.gov.ua/laws/show/2657-12?find (accessed 24 February 2021).

22.ISACA International (2015, January). *Global Cybersecurity Status Repor*. [online] Available at: www.isaca.org/cyber/ Documents/2015-Global-Cybersecurity-StatusReport-Data-Sheet_ mkt_Eng_0115.pdf (accessed 24 February 2021).

**Ph.D. in Economics, Associate Professor Gorodianska L.V., Tsiukalo L.V.**

## INFORMATION SECURITY OF SMALL BUSINESSES IN THE CONTEXT OF DIGITALIZATION

***The article defines and analyzes the characteristic features of modern society digitalization, in particular the digital economy. It is noted that progress in the digital technology environment requires the application of information security measures, primarily in the financial and economic activities of small businesses. The interpretation of the definitions «information security» and «economic security» has been clarified. Attention is drawn to a conscious understanding of the interaction between people and technology during the digital transformation of the economy in such a way that the latest technologies must adapt to people, and not vice versa. It is emphasized that such an understanding can come only in the process of training and acquiring appropriate professional competencies, especially among small businesses. The types of small businesses information that are subject to protection and components of economic security are determined. Proposals have been formed for the creation of a comprehensive security program, which should include an action plan aimed at protecting the functioning of the enterprise's information system from external and internal influences, and a set of measures designed to protect the confidentiality, availability, and integrity of data from internal and external, malicious and accidental threats. Information security of small businesses in the context of digitalization should be based on the following positions: the management of the enterprise should regularly train all employees in the principles of Information Security, data protection and protect physical data carriers from cyber attacks; the corporate network should be segmented, and access to it – controlled; partnership with service providers from the point of view of information security should be equivalent; remote access to the corporate network of the enterprise, which is now becoming more widespread, should be as secure as possible and comply with information security standards.***

***A promising area of further research is the development of a set of measures at the state level, which includes streamlining the simplified tax system, promoting the development of innovative entrepreneurship, cluster organization of small businesses, the formation of a modern information infrastructure to support entrepreneurship, the formation of a favorable business climate.***

***Keywords: digitalization, digital technology, digital economy, small business entity, information security, economic security, information protection.***