

---

**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

---

DOI: [https://doi.org/10.25140/2410-9576-2024-1\(28\)-208-223](https://doi.org/10.25140/2410-9576-2024-1(28)-208-223)

УДК 004.056.5:[004.738.5:339

JEL Classification: L81

**Максим Вікторович Дубина**

доктор економічних наук, професор,  
завідувач кафедри фінансів, банківської справи та страхування  
Національний університет «Чернігівська політехніка» (Чернігів, Україна)  
E-mail: [maksim-32@ukr.net](mailto:maksim-32@ukr.net). ORCID: <https://orcid.org/0000-0002-5305-7815>  
ResearcherID: [F-3291-2014](https://orcid.org/0000-0002-5305-7815). Scopus Author ID: [56912277800](https://orcid.org/0000-0002-5305-7815)

**Олексій Володимирович Заєць**

аспірант кафедри фінансів, банківської справи та страхування  
Національний університет «Чернігівська політехніка» (Чернігів, Україна)  
E-mail: [oleksijzaec82@ukr.net](mailto:oleksijzaec82@ukr.net). ORCID: <https://orcid.org/0009-0000-7974-0009>

**ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ  
ПІДПРИЄМСТВ ЕЛЕКТРОННОЇ КОМЕРЦІЇ  
В УМОВАХ СТАНОВЛЕННЯ ЦИФРОВОЇ ЕКОНОМІКИ**

**Анотація.** У статті поглиблено теоретичні положення обґрунтування особливостей забезпечення кібербезпеки підприємств електронної комерції в умовах становлення цифрової економіки. Це було реалізовано через розгляд сучасного стану розвитку електронної комерції у світі та визначення передумов подальшого розвитку цієї галузі. Обґрунтовано особливості економічної діяльності підприємств електронної комерції та вплив специфіки їх господарської діяльності на формування систем інформаційної безпеки цих підприємств. Також проаналізовано причини необхідності здійснення захисту інформаційних систем суб'єктів господарювання від зовнішнього втручання в сучасних умовах цифровізації національної економіки. У підсумку виокремлено передумови створення системи кібербезпеки підприємствами електронної комерції та конкретизовано загальні заходи підвищення ефективності її функціонування у роботі таких підприємств.

**Ключові слова:** електронна комерція, кібербезпека, цифровізація, система кіберзахисту, підприємство електронної торгівлі, цифрова економіка, інформаційна безпека.

Рис.: 4. Бібл.: 16.

**Постановка проблеми.** Сучасні процеси цифровізації є об'єктивними з позиції функціонування економічних систем. Значний розвиток цифрових технологій сьогодні сприяє їх трансформації, включаючи й діяльність економічних суб'єктів. Такі суб'єкти намагаються адаптуватися під нові зовнішні умови таким чином, щоб максимально використати потенціал інформаційно-комунікаційних технологій у власній діяльності, мінімізуючи негативні наслідки їх застосування.

---

**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

---

Завдяки активному розвитку інформаційних технологій у структурі національної економіки багатьох країн з'явилися нові напрями економічної діяльності, які в підсумку сформували окремі галузі, сектори, підгалузі національного господарства. Значна кількість підприємств у сучасному світі здійснюють свою діяльність виключно завдяки використанню цифрових технологій. Відповідно, підприємства електронної комерції можна віднести до таких суб'єктів господарювання. Ці економічні суб'єкти виникли й розвиваються в унісон з основними напрями становлення інформаційного суспільства, яке у свою чергу функціонує і розвивається відповідно до використання цифрових технологій у діяльності різних соціальних та економічних систем.

Саме активний розвиток підприємств електронної комерції в усьому світі зумовлює пошук їхніми власниками нових способів розширення діяльності. У сучасних умовах це здебільшого вже здійснюється за допомогою використання сучасних цифрових технологій. Такі підприємства намагаються постійно змінюватися та застосовувати сучасні інновації у сферах продажу, обслуговування клієнтів. Проте цифровізація також сприяє і виникненню нових загроз для діяльності підприємств електронної комерції, і це також вимагає відповідних дій з боку власників та топменеджменту цих підприємств. Особливо складною у цифровому світі стає ситуація із забезпеченням інформаційної безпеки для всіх суб'єктів господарювання. Отже, окреслене актуалізує питання теоретичного обґрунтування ролі кібербезпеки в розвитку підприємств електронної комерції.

**Аналіз останніх досліджень і публікацій.** Питання розвитку підприємств електронної комерції сьогодні активно досліджуються науковцями. Серед них насамперед варто виокремити таких: К. Краус, А. В. Алфімова, О. Ю. Засенко, Г. О. Манорик, Я. С. Тертичний, Г. Тітова, В. В. Фалдина та ін.

Особливості формування системи кіберзахисту цих суб'єктів господарювання в умовах становлення цифрової економіки розглядали у своїх роботах М. Д. Василенко, Н. С. Кирєєва, Є. В. Кочура, І. М. Пістунов, П. Романюк, О. Харченко, В. Р. Яремич та ін.

---

**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

---

**Виділення недосліджених частин загальної проблеми.** Проте, незважаючи на численні напрацювання вчених у напрямку розвитку електронної комерції, питання забезпечення їх інформаційної безпеки, її впливу на їхню господарську діяльність, формування ефективних систем кібербезпеки цих суб'єктів господарювання залишаються актуальними й потребують додаткового вивчення та поглиблення.

**Метою статті** є теоретичне обґрунтування особливостей забезпечення кібербезпеки підприємств електронної комерції в умовах становлення цифрової економіки.

**Виклад основного матеріалу.** Підприємства електронної комерції у свій час стали не лише тими економічними суб'єктами, які активно використовували інформаційні технології, але в багатьох випадках ставали центрами створення нових інформаційно-комунікаційних технологій. Такі технології вже в подальшому активно використовували та адаптували під свою діяльність інші економічні суб'єкти. Така ситуація цілком зрозуміла, враховуючи, що ефективність використання інформаційно-комунікаційних технологій у діяльності підприємства електронної комерції визначає і загалом ефективність їхньої роботи. Саме тому ці економічні суб'єкти значну увагу й у минулому, і сьогодні приділяють створенню і адаптації сучасних цифрових технологій до своєї діяльності, власних бізнес-процесів, які ними впроваджуються для підтримки економічної діяльності, забезпечення стабільного функціонування та розвитку бізнесу. І роль таких суб'єктів господарювання у стимулюванні та підтримці процесів цифровізації економічних систем буде лише поглиблюватися, що зумовлено активним розвитком усієї галузі електронної комерції у світі та постійно зростаючим попитом на послуги підприємств, які здійснюють свою діяльність у цій галузі. На рис. 1 представлено інформацію про сучасний розвиток підприємств електронної комерції.

Таким чином з даних рис. 1 можна зробити висновок про досить динамічний розвиток підприємств електронної комерції у світі. Наприклад у сфері ритейлу у 2024 р. прогнозується зростання продажів до 6,36 трлн дол. США. З урахуванням, що ще у 2020 р. цей показник складав лише 4,28 трлн дол. США.

## УПРАВЛІННЯ ПІДПРИЄМСТВОМ

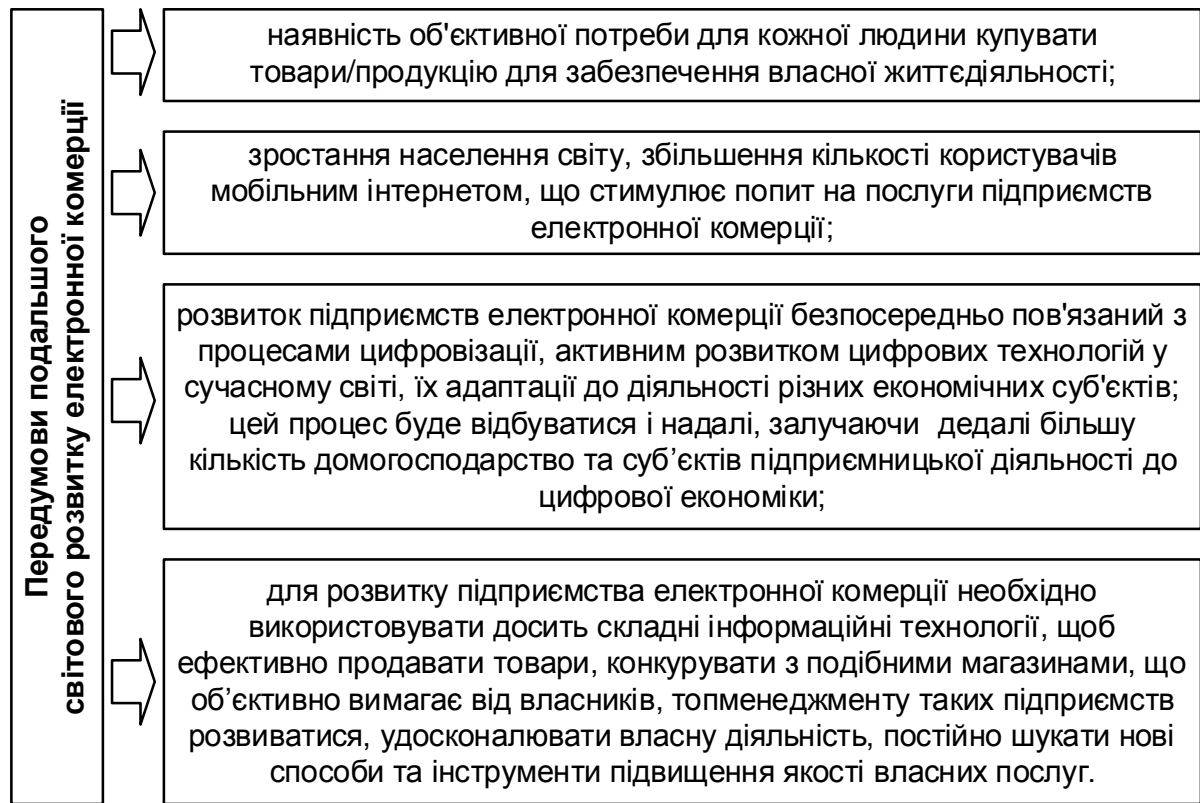


**Рис. 1. Інформація про розвиток підприємств електронної комерції у світі**

*Джерело: Statista [14; 15].*

Проникнення цифрових технологій у всі сфери економічного життя сучасного суспільства сьогодні продовжує здійснювати досить стрімкий вплив на розвиток підприємств електронної комерції. З одного боку, таке проникнення супроводжується поступовим зростанням цифрової грамотності громадян, що безпосередньо впливає на залучення їх і до системи електронної торгівлі. З іншого боку, саме COVID-19 став досить потужним імпульсом до розвитку електронної комерції в усьому світі. Активніше почали розвиватися і економічні суб'єкти, які надають послуги підприємствам електронної комерції, підтримують їхню діяльність. До цієї сфери почали долучатися навіть ті підприємства, які дотримувалися традиційної бізнес-моделі, а саме продажу товарів у фізичних магазинах. Поступово наявність онлайн-магазинів стало не лише бажаним для забезпечення зростання продажів, але й фактично обов'язковим для торговельних підприємств, які повинні підтримувати власну репутацію та належний рівень цифрового розвитку й конкурентоспроможності. Сьогодні існують усі передумови для подальшого світового розвитку електронної комерції і відповідно процесу цифрової трансформації цієї галузі (рис. 2).

## УПРАВЛІННЯ ПІДПРИЄМСТВОМ



**Рис. 2. Передумови подальшого світового розвитку електронної комерції**

*Джерело: складено авторами з урахуванням [16].*

Розвиток підприємств електронної комерції зумовлений як зовнішніми чинниками, які загалом впливають на розвиток значної кількості економічних суб'єктів, так і внутрішніми факторами, які виникають безпосередньо в межах сфери електронної комерції і пов'язані в першу чергу з ринковими факторами. Вплив цих чинників переважно є постійним та одночасним, що вимагає від підприємств електронної комерції врахування наслідків їхнього впливу, впровадження механізмів протидії негативним наслідкам від такого впливу. У межах діяльності такого підприємства це можливо зробити виключно через постійне вдосконалення інформаційних систем, які ними використовуються. Втрата даних клієнтів, комерційної інформації негативно впливають не лише на фінансові витрати, але і негативно впливають на їхню репутацію серед клієнтів, партнерів, постачальників товарів та послуг. Це своєю чергою зумовлює використання сучасних цифрових технологій не лише у сфері

---

**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

---

надання власних послуг клієнтам, продажу товарів, але також і у сфері власної інформаційної безпеки. Окреслене актуалізує питання пошуку методів, інструментів забезпечення належного рівня такої безпеки, побудови дійсно ефективної системи кібербезпеки.

Сучасний етап розвитку кібербезпеки характеризується новими тенденціями, які пов'язані з переходом від кількісного до якісного зростання стану технічного забезпечення самої інформаційної технології. Водночас сама кібербезпека реалізує стан захищеності інтересів як держави й суспільства загалом, так і кожного окремого індивіда від кіберзагроз. Фактично це правове, організаційне, науково-технічне, інформаційне забезпечення мережевої та комп'ютерної безпеки. Кібербезпека спрямована на забезпечення ефективного захисту кіберпростору та включає, зокрема, криптографічний захист інформації, адміністративну та інформаційну безпеку інформаційно-телекомунікаційних систем, безпеку вебсайтів [2, с. 29].

У сучасних умовах необхідність захисту інформаційної системи від потенційного зовнішнього негативного втручання в її функціонування зумовлена такими причинами:

– постійне зростання кількості кібератак на функціонування підприємств, які здійснюють активну діяльність в мережі інтернет, підвищення якості таких кібератак, що вимагає постійного пошуку нових методів та інструментів для як запобігання таким атакам, так і впровадження механізмів протидії їм;

– необхідність постійного оновлення інформаційної системи підприємства через активний розвиток цифрових технологій, підвищення вимог клієнтів до зручності використання сайтів, додатків таких підприємств;

– загострення конкуренції, зростання кількості випадків недобросовісної конкуренції, що вимагає також постійного удосконалення інформаційної системи;

– впровадження нових цифрових технологій у діяльність підприємств може потенційно в короткостроковій перспективі негативно впливати на рівень їх інформаційної безпеки через впровадження нової системи кіберзахисту, її адаптацію до умов діяльності такого підприємства.



---

**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

---

Розглянемо детальніше особливості ведення бізнесу підприємствами електронної комерції, які загалом і визначають специфічні риси побудови стабільно функціонуючої системи їх кіберзахисту. До таких особливостей, на наше переконання, належать такі:

- необхідність незначних інвестицій для початку здійснення діяльності у сфері електронної комерції (для малих підприємств);
- необхідність підтримувати всі бізнес-процеси в онлайн режимі, а отже, працювати з великими обсягами інформації;
- спрощена система оподаткування невеликих магазинів, які надають свою діяльність виключно в онлайн-форматі;
- залежність від розвитку фінансових установ і відповідно функціонування платіжних систем;
- залежність від роботи інших економічних суб'єктів, їх стабільного функціонування (логістичні компанії, компанії з доставки товарів оптові продавці, телекомунікаційні компанії);
- необхідність залучення висококваліфікованих фахівців, робота яких є високооплачуваною для підтримки роботи онлайн-магазинів, обслуговування клієнтів;
- враховуючи, що значна кількість підприємств електронної комерції є невеликими магазинами, то гнучкість їхньої роботи та можливості адаптації до змінного зовнішнього середовища є на порядок вищими, рішення ухвалюються оперативніше відповідно до ситуації, яка складається на окремих ринках товарів;
- висока конкуренція на ринках товарів та продукції, значна кількість електронних магазинів, підприємств, які суміщають продаж товарів в офлайн і в онлайн режимах;
- доступ до світового ринку товарів, продукції, послуг та сировини, які підприємства електронної комерції мають змогу замовляти для підприємницької діяльності у всьому світі;
- доступу до світових ринків, що дозволяє підприємствам електронної комерції шукати покупців, клієнтів у всьому світі; це дозволяє розширити бізнес, використовувати аутсорсингові послуги від компанії з усього світу для підтримки власної діяльності (наприклад, ІТ-підтримка, фінансові послуги);

**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

– необхідність використання сучасних інформаційно-комунікаційних технологій у всіх напрямках ведення бізнесу, включаючи маркетинг, логістичну діяльність, консультаційну діяльність, управління персоналом [1, с. 62; 6; 8, с. 215; 11; 10, с. 71-73].

На рис. 3 представлено інформацію про опитування бізнес-лідерів та фахівців у сфері кібербезпеки щодо можливих втрат від нових кібератак.



**Рис. 3. Результати опитування основних, особистих занепокоєнь бізнес-лідерів щодо кібербезпеки**

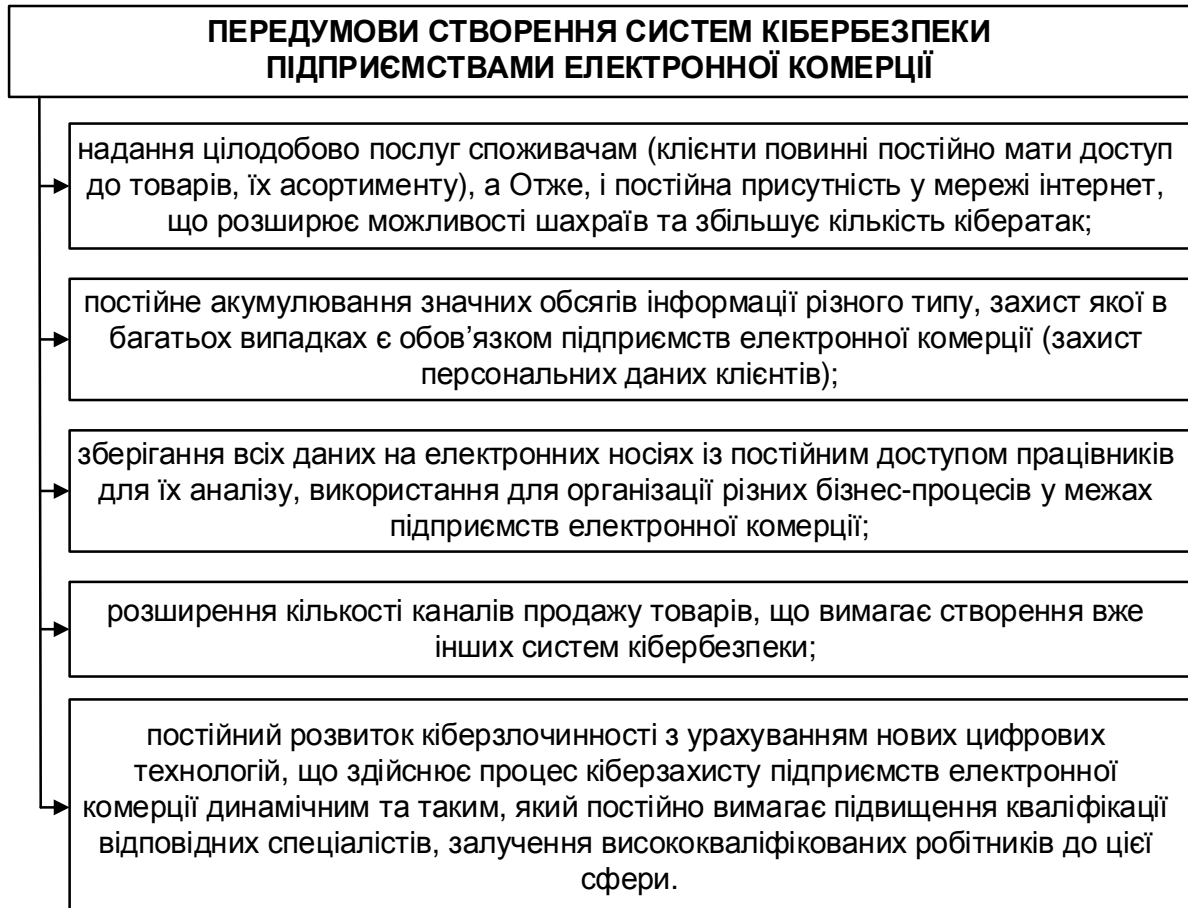
*Джерело: [13].*

Більшість опитаних зазначили, що найскладнішими будуть наслідки від кібератак, які вплинуть на окремі бізнес-процеси на підприємстві, що призведе до зупинення його операційної діяльності і може призвести до значних фінансових витрат. Також значна кількість топ-лідерів вважають саме кібервимагання небезпечним для бізнесу, оскільки настання таких ризиків приводить до фінансових витрат і зниженню репутації підприємств.



**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

Об'єктивність потреби в забезпеченні високого рівня кібербезпеки підприємств електронної комерції також зумовлена низкою передумов та причин (рис. 4).



**Рис. 4. Передумови створення систем кібербезпеки підприємствами електронної комерції**

*Джерело: складено авторами на основі [3; 5; 7; 11, с. 209].*

Також однією з важливих особливостей забезпечення надійності інформаційної системи підприємств електронної комерції є об'єктивна їх потреба у взаємодії з іншими економічними суб'єктами для здійснення своєї діяльності. Особливо серед таких суб'єктів варто виокремити фінансові компанії, їх співпрацю з підприємствами електронної комерції, реалізацію спільних програм кредитування, кооперація для забезпечення можливостей клієнтів купувати зараз, навіть якщо тимча-

---

**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

---

сово власних коштів не вистачає. У багатьох випадках на сайтах онлайн-магазинів можна зробити заявку на отримання кредиту. Без того онлайн-магазини досить часто створюють свої системи онлайн-платежів, акумулюють і відповідно фінансову інформацію клієнтів.

Отже, у сучасних умовах становлення цифрової економіки для підвищення ефективності функціонування власної системи кібербезпеки підприємства електронної комерції можуть здійснити наступне:

1) поглиблення співпраці з органами державної влади, відповідними державними інститутами, які займаються боротьбою з кіберзлочинністю; залучення до роботи колишніх працівників цих органів;

2) поступово формувати команду кваліфікованих працівників у сфері кіберзахисту, що вимагає здійснення додаткових витрат;

3) активне використання сучасних технологій для автоматичного виявлення та попередження нових кібератак (використання технології штучного інтелекту, інші методи автоматизації роботи з інформаційними даними);

4) обов'язкове збереження копії всієї інформаційної системи, її компонентів за допомогою використання хмарних технологій;

5) уважний перегляд системи доступу працівників до різних типів управлінської та аналітичної інформації;

6) поступове впровадження системи кіберзахисту в діяльність підприємства електронної комерції, яка полягала у глибокому проникненні інструментів захисту інформації, її доступу, особливостей використання на всіх етапах та в усіх підрозділах функціонування такого підприємства;

7) розробка та поступове впровадження стратегії кіберзахисту підприємства електронної комерції в довгостроковій перспективі, акцент на постійності здійснення захисту, впровадженні довгострокових заходів для його забезпечення, а не досягнення виключно тактичних цілей;

8) активне використання технології аутсорсингу та залучення необхідних фахівців;

9) активне використання шифрування даних, багатофакторної аутентифікації;

10) періодично проводити аналіз кіберзахисту за допомогою залучення зовнішніх спеціалістів та ін. [2; 9, с. 181; 12].

---

**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

---

**Висновки та пропозиції.** Отже, детальний розгляд теоретичних положень забезпечення кібербезпеки підприємств електронної комерції в умовах становлення цифрової економіки дозволило виокремити специфічні риси діяльності таких суб'єктів господарювання, визначити потенціал їхнього розвитку та конкретизувати специфічні риси забезпечення інформаційної безпеки таких підприємств. Результати проведеного дослідження засвідчують, що в сучасному світі, у якому активно розвиваються інформаційно-комунікаційні технології, є об'єктивна необхідність у побудові дієвих систем кіберзахисту діяльності економічних суб'єктів. При цьому підприємства, до яких доцільно віднести й суб'єктів господарювання, що здійснюють свою діяльність у галузі електронної комерції, які функціонують на основі використання інформаційних цифрових технологій об'єктивно для власного виживання і забезпечення конкурентоспроможності зобов'язані розробляти, використовувати та впроваджувати методи та інструменти боротьби з кіберзагрозами й іншими інформаційними ризиками, з якими вони можуть зіштовхнутися у своїй роботі.

У статті визначено, що специфіка економічної діяльності підприємств електронної комерції вимагає від них організації ефективної системи інформаційного забезпечення всіх бізнес-процесів, які відбуваються в межах функціонування такого підприємства. Таким чином, зазначені суб'єкти господарювання зобов'язані в процесі розробки і впровадження власної стратегії розвитку враховувати питання забезпечення кіберзахисту, розробляти відповідні стратегічні та тактичні цілі і заходи їх досягнення для підвищення власного рівня інформаційної безпеки. Також встановлено, що в сучасних умовах розвиток підприємств електронної комерції нерозривно пов'язаний з ефективністю функціонування їхніх систем кіберзахисту і саме надійність інформаційних систем дає змогу забезпечити не лише продуктивність внутрішніх процесів, які притаманні бізнес-діяльності, але й формує умови для зростання довіри діючих та потенційних клієнтів, покращення репутації підприємств електронної комерції та підвищення рівня їх конкурентоспроможності на висококонкурентних світових ринках товарів, послуг, сировини та капіталу. Запропоновані у статті напрямки підвищення ефективності функціонування системи кібербезпеки підприємств електронної комерції є пріоритетними для їх ви-

---

**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

---

користання. Їх поступове виконання дозволить підвищити рівень кіберзахисту таких підприємств, але не гарантує цілковиту інформаційну безпеку для них, оскільки інформаційний простір, у якому всі суб'єкти господарювання сьогодні розвиваються, постійно змінюється, також постійно удосконалюються технології та методи здійснення кібершахрайства та проникнення в діяльність економічних суб'єктів включаючи підприємства електронної комерції.

**Список використаних джерел**

1. Алфімова А. В. Стратегічний розвиток системи електронної комерції в Україні [Електронний ресурс] : дис. ... канд. екон. наук : спец. 08.00.03 «Економіка та управління національним господарством» / Міжнародний науково-технічний університет імені академіка Юрія Бугая; Класичний приватний університет. – Запоріжжя, 2021. – 212 с. – Режим доступу: [http://virtuni.education.zp.ua/info\\_cpu/sites/default/files/dis\\_Alfimova.pdf](http://virtuni.education.zp.ua/info_cpu/sites/default/files/dis_Alfimova.pdf).

2. Василенко М. Д. Електронна комерція у проявах юриспруденції (законодавства) та кібербезпеки (несанкціонованих вторгнень): міждисциплінарне дослідження [Електронний ресурс] / М. Д. Василенко, Н. С. Киреєва // Наукові праці НУ ОЮА. – 2020. – № 26. – С. 25-33. – Режим доступу: <http://naukovipraci.nuoua.od.ua/arhiv/tom26/6.pdf>.

3. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест [Електронний ресурс] / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В. І. Вернадського. – Київ, 2024. – № 3 (березень). – 339 с. – Режим доступу: <https://ippi.org.ua/sites/default/files/2024-3.pdf>.

4. Кіберзлочинність та електронні докази = Cybercrime and digital evidence [Електронний ресурс] : навч. посібник / [Б. М. Головін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. – Електрон. вид. – Львів : ЛНУ ім. Івана Франка, 2022. – 298 с. – (Удосконалення магістер. програми з кримін. юстиції = Modernising Master's Training on Criminal Justice. CRIMHUM). – Режим доступу: <https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf>.

5. Пістунов І. М. Безпека електронної комерції [Електронний ресурс] : навч. посіб. / І. М. Пістунов, Є. В. Кочура ; Нац. гірн. ун-т. – Д. : НГУ, 2014. – 125 с. – Режим доступу: [http://pistunovi.narod.ru/6\\_E\\_K.pdf](http://pistunovi.narod.ru/6_E_K.pdf).

6. Романюк П. Основні проблеми електронної комерції в умовах цифрової трансформації бізнесу [Електронний ресурс] / П. Романюк // Цифрова економіка та економічна безпека. – 2023. – № 4(04). – С. 32-37. – Режим доступу: <http://dees.iei.od.ua/index.php/journal/article/view/125>.

7. Садчикова І. Теоретичне обґрунтування сутності поняття «електронна комерція» / І. Садчикова, А. Тарасенко, М. Дубина // Економіка та суспільство. – 2023. – № 53. – DOI: <https://doi.org/10.32782/2524-0072/2023-53-36>.

---

**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

---

8. Скопенко Н. С. Використання електронної комерції як напрям зменшення ризиковості бізнесу та створення конкурентної переваги [Електронний ресурс] / Н. С. Скопенко, Ю. В. Поліщук // Інфраструктура ринку. – 2021. – № 51. – С. 214–219. – Режим доступу: [http://www.market-infr.od.ua/journals/2021/51\\_2021\\_ukr/36.pdf](http://www.market-infr.od.ua/journals/2021/51_2021_ukr/36.pdf).

9. Столбовий В. М. Заходи з підвищення кібербезпеки на державному та корпоративному рівнях в умовах діджиталізації суспільства / В. М. Столбовий, Д. П. Кисленко // Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична. – 2023. – Вип. 37. – С. 175-183.

10. Фалдина В. В. Розвиток підприємницьких структур на основі технологій електронної комерції [Електронний ресурс] : дис. ... канд. екон. наук : спец. 08.00.04 «Економіка та управління підприємствами (за видами економічної діяльності)» / Львівський університет бізнесу та права. – Львів, 2021. – 206 с. – Режим доступу: [https://lubp.com.ua/wp-content/uploads/2017/04/%D0%94%D0%B8%D1%81%D0%B5%D1%80%D1%82%D0%B0%D1%86%D1%96%D1%8F\\_\\_%D0%A4%D0%B0%D0%BB%D0%B4%D0%B8%D0%BD%D0%B0.pdf](https://lubp.com.ua/wp-content/uploads/2017/04/%D0%94%D0%B8%D1%81%D0%B5%D1%80%D1%82%D0%B0%D1%86%D1%96%D1%8F__%D0%A4%D0%B0%D0%BB%D0%B4%D0%B8%D0%BD%D0%B0.pdf).

11. Харченко О. Модель впровадження технологій електронної комерції [Електронний ресурс] / О. Харченко, В. Яремич // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – 2023. – № 2(22). – С. 204–213. – Режим доступу: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/543>.

12. CYBER DIGEST. Огляд подій в сфері кібербезпеки, липень 2023 [Електронний ресурс]. – Режим доступу: [https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/2023/Cyber%20digest\\_July\\_2023\\_UA.pdf](https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/2023/Cyber%20digest_July_2023_UA.pdf).

13. Global Cybersecurity. Outlook 2024. INSIGHT REPORT. – JANUARY 2024 [Electronic resource]. – Accessed mode: [https://www3.weforum.org/docs/WEF\\_Global\\_Cybersecurity\\_Outlook\\_2024.pdf](https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf).

14. Mosby A. Global eCommerce Sales Growth (2016 – 2027) [Electronic resource] / Albert Mosby // Yaguara. – March 12, 2024. – Accessed mode: <https://www.yaguara.co/global-ecommerce-sales-growth>.

15. Retail e-commerce sales worldwide from 2014 to 2027 [Electronic resource] // Statista. – 2024. – Accessed mode: <https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales>.

16. The Role of Digitalization in Ensuring the Financial and Economic Security of Trading Enterprises Under the Conditions of External Shocks [Electronic resource] / M. Dubyna, L. Verbivska, O. Kalchenko, V. Dmytrovska, D. Pilevych, I. Lysohor. // International Journal of Safety and Security Engineering. – 2023. – Vol. 13, No. 5. – Pp. 821-833. – Accessed mode: <https://www.iieta.org/journals/ijssse/paper/10.18280/ijssse.130506>.

## References

1. Alfimova, A.V. (2021). *Stratehichniy rozvytok systemy elektronnoi komertsii v Ukraini [Strategic development of the electronic commerce system in Ukraine]* [PhD dissertation; Mizhnarodnyi naukovy-tekhnichnyi universytet imeni akademika Yuriiia Buhaia; Klasychnyi pryvatnyi uni-versytet]. [http://virtuni.education.zp.ua/info\\_cpu/sites/default/files/dis\\_Alfimova.pdf](http://virtuni.education.zp.ua/info_cpu/sites/default/files/dis_Alfimova.pdf).



---

**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

---

2. Vasylenko, M.D., Kyreieva, N.S. (2020). Elektronna komertsiiia u proiavakh yurysprudentsii (zakono-davstva) ta kiberbezpeky (nesanktsionovanykh vtorhnen): mizhdystsyplinarne doslidzhennia [Electronic commerce in manifestations of jurisprudence (legislation) and cyber security (unauthorized intrusions): interdisciplinary research]. *Naukovi pratsi NU OluA – Scientific works of the National Academy of Sciences of Ukraine*, (26), 25-33. <http://naukovipraci.nuoua.od.ua/arhiv/tom26/6.pdf>.
3. Dovhan, O. (Ed.). (2024). *Kiberbezpeka v informatsiinomu suspilstvi: Informatsiino-analitychnyi daidzhest [Cybersecurity in the information society: Informational and analytical digest]*, 3(March). <https://ippi.org.ua/sites/default/files/2024-3.pdf>.
4. Denkovich, O., Shmeltser, H. (2022). *Kiberzlochynnist ta elektronni dokazy = Cybercrime and digital evidence [Cybercrime and digital evidence]*. LNU im. Ivana Franka. (Modernising Master's Training on Criminal Justice. CRIMHUM). <https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf>.
5. Pistunov, I.M., Kochura, Ye.V. (2014). *Bezpeka elektronnoi komertsii [Security of electronic commerce]*. NHU. [http://pistunovi.narod.ru/6\\_E\\_K.pdf](http://pistunovi.narod.ru/6_E_K.pdf).
6. Romaniuk, P. (2023). Osnovni problemy elektronnoi komertsii v umovakh tsyfrovoy transformatsii biznesu [The main problems of e-commerce in the conditions of digital transformation of business]. *Tsyfrova ekonomika ta ekonomichna bezpeka – Digital economy and economic security*, 4(04), 32-37. <http://dees.iei.od.ua/index.php/journal/article/view/125>.
7. Sadchykova, I., Tarasenko, A., Dubyna, M. (2023). Teoretychne obgruntuvannia sutnosti poniattia «elektronna komertsiiia» [Theoretical justification of the essence of the concept of "electronic commerce"]. *Ekonomika ta suspilstvo – Economy and society*, (53). <https://doi.org/10.32782/2524-0072/2023-53-36>.
8. Skopenko, N.S., Polishchuk, Yu.V. (2021). Vykorystannia elektronnoi komertsii yak napriam zmenshen-nia ryzykovosti biznesu ta stvorennia konkurentnoi perevahy [The use of electronic commerce as a way of reducing business risk and creating a competitive advantage]. *Infrastruktura rynku – Market infrastructure*, (51), 214–219. [http://www.market-infr.od.ua/journals/2021/51\\_2021\\_ukr/36.pdf](http://www.market-infr.od.ua/journals/2021/51_2021_ukr/36.pdf).
9. Stolbovyi, V.M., Kyslenko, D.P. (2023). Zakhody z pidvyshchennia kiberbezpeky na derzhavnomu ta korporatyvnomu rivniakh v umovakh didzhetalizatsii suspilstva [Measures to increase cyber security at the state and corporate levels in the conditions of digitalization of society]. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava. Serii ekonomichna. Serii yurydychna – Scientific notes of the Lviv University of Business and Law. Economic series. Legal series*, 37, 175-183.
10. Faldyna, V.V. (2021). *Rozvytok pidpriemnytskykh struktur na osnovi tekhnolohii elektronnoi komertsii [Development of entrepreneurial structures based on electronic commerce technologies]* [PhD dissertation; Lvivskyi universytet biznesu ta prava]. [https://lubp.com.ua/wp-content/uploads/2017/04/%D0%94%D0%B8%D1%81%D0%B5%D1%80%D1%82%D0%B0%D1%86%D1%96%D1%8F\\_\\_%D0%A4%D0%B0%D0%BB%D0%B4%D0%B8%D0%BD%D0%B0.pdf](https://lubp.com.ua/wp-content/uploads/2017/04/%D0%94%D0%B8%D1%81%D0%B5%D1%80%D1%82%D0%B0%D1%86%D1%96%D1%8F__%D0%A4%D0%B0%D0%BB%D0%B4%D0%B8%D0%BD%D0%B0.pdf).



---

**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

---

11. Kharchenko, O., Yaremych, V. (2023). Model vprovadzhennia tekhnolohii elektronnoi komertsii [Model of implementation of electronic commerce technologies]. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika» – Electronic professional scientific edition "Cybersecurity: education, science, technology"*, 2(22), 204–213. <https://csecurity.kubg.edu.ua/index.php/journal/article/view/543>.

12. CYBER DIGEST. Огляд подій в сфері кібербезпеки, липень 2023 [CYBER DIGEST. Review of events in the field of cyber security, July 2023]. (2024). [https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/2023/Cyber%20digest\\_July\\_2023\\_UA.pdf](https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/2023/Cyber%20digest_July_2023_UA.pdf).

13. Global Cybersecurity. Outlook 2024. INSIGHT REPORT. (January 2024). [https://www3.weforum.org/docs/WEF\\_Global\\_Cybersecurity\\_Outlook\\_2024.pdf](https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf).

14. Mosby, A. (March 12, 2024). *Global eCommerce Sales Growth (2016 – 2027)*. Yaguara. <https://www.yaguara.co/global-ecommerce-sales-growth>.

15. *Statista*. (2024). Retail e-commerce sales worldwide from 2014 to 2027. <https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales>.

16. Dubyna, M., Verbivska, L., Kalchenko, O., Dmytrovska, V., Pilevych, D., Lysohor, I. (2023). The Role of Digitalization in Ensuring the Financial and Economic Security of Trading Enterprises Under the Conditions of External Shocks. *International Journal of Safety and Security Engineering*, 13(5), 821-833.

Отримано 26.01.2024

UDC 004.056.5:[004.738.5:339

JEL Classification: L81

### **Maksym Dubyna**

Doctor of Economics, Professor, Head of the Department of Finance, Banking and Insurance Chernihiv Polytechnic National University (Chernihiv, Ukraine)

**E-mail:** [maksim-32@ukr.net](mailto:maksim-32@ukr.net). **ORCID:** <http://orcid.org/0000-0002-5305-7815>

**ResearcherID:** [F-3291-2014](https://orcid.org/0000-0002-5305-7815). **Scopus Author ID:** [56912277800](https://orcid.org/0000-0002-5305-7815)

### **Oleksii Zaiets**

PhD Student, Department of Finance, Banking and Insurance Chernihiv Polytechnic National University (Chernihiv, Ukraine)

**E-mail:** [oleksijzaec82@ukr.net](mailto:oleksijzaec82@ukr.net). **ORCID:** <https://orcid.org/0009-0000-7974-0009>

## **ENSURING CYBER SECURITY OF E-COMMERCE ENTERPRISES IN THE CONDITIONS OF THE EMERGING DIGITAL ECONOMY**

**Abstract.** *Active development of e-commerce enterprises in the world is driving their owners to look for new ways to expand their activities. In the conditions of the current environment, this is already being done in the vast majority of cases using modern digital technologies. These companies try to constantly changing and applying modern innovations in sales, customers' service. However, digitalization also contributes to the emergence of new threats to e-*

---

**УПРАВЛІННЯ ПІДПРИЄМСТВОМ**

---

commerce businesses, and appropriate actions are required by the owners and top management of these enterprises. One of the challenges facing the e-commerce enterprises today is available cyber threats and external interference in the works of these enterprises through the information system to ensure the conduct of economic activities.

In the article, theoretical provisions to substantiate the peculiarities of cybersecurity of e-commerce enterprises in the context of the digital economy formation and the impact of the specifics of their economic activity on the formation of information security systems of these enterprises are deepened. It is also established that in modern conditions, development of the e-commerce enterprises is inextricably linked to effective operation of their cyber security systems, and it is the reliability of information systems that allows both ensuring productivity of internal processes, and creating the conditions to increase the trust of existing and potential customers, improving reputation of the e-commerce enterprises and their competitiveness increase.

Therefore, the prerequisites for establishing the cybersecurity system by e-commerce enterprises are highlighted, and common measures to improve the efficiency of its functioning in the operation of these enterprises are specified. Their gradual implementation will increase the cybersecurity level, but does not guarantee safe information security for them, since the information space where all business entities develop today, is constantly changing, and technologies and methods of the cyber fraud and penetration into the activities of economic entities, including e-commerce enterprises, are constantly developing.

**Keywords:** e-commerce, cyber security, cybersecurity system, e-commerce enterprise, digital economy, information security.

Fig.: 4. References: 16.

**Бібліографічний опис для цитування:**

Дубина М. В., Заєць О. В. Забезпечення кібербезпеки підприємств електронної комерції в умовах становлення цифрової економіки. *Науковий вісник Полісся*. 2024. № 1(28). С. 208-223.