УДК: 004.056:005.574 DOI: https://doi.org/10.32680/2409-9260-2025-7-8-332-333-146-154

ЦИФРОВА БЕЗПЕКА ДІЛОВИХ ПЕРЕГОВОРІВ

Бондаренко О. М., кандидат філософських наук, доцент, доцент кафедри маркетингу та міжнародної логістики, Одеський національний економічний університет, м. Одеса, Україна
e-mail: 7871996@gmail.com
ORCID: 0000-0001-9853-5051

Бондаренко Л. Г., викладач відокремленого структурного підрозділу «Фаховий коледж зв'язку та інформатизації Державного університету інтелектуальних технологій і зв'язку», м. Одеса, Україна
e-mail: liliiabondarenk@gmail.com
ORCID: 0009-0003-8984-5420

Анотація. *Метою дослідження є визначення сутності цифрової безпеки ділових переговорів, виявлення основних кіберзагроз та обґрунтування комплексу технічних, організаційних і психологічних заходів захисту конфіденційної інформації в умовах цифровізації бізнес-комунікацій. Методика дослідження базується на структурно-логічному аналізі, порівнянні сучасних практик кіберзахисту, узагальненні наукових публікацій та матеріалів періодики. Результати дослідження показують, що цифрова безпека переговорів поєднує технічні (шифрування, VPN, контроль доступу), організаційні (політика конфіденційності, перевірка партнерів) та людські аспекти (навчання кібергігієні, протидія соціальній інженерії). Основні загрози – несанкціонований доступ, викрадення даних, маніпуляції інформацією та фішинг. Комплексні рішення значно підвищують стійкість переговорів до зовнішніх атак і внутрішніх ризиків. Практична значущість дослідження полягає у можливості застосування результатів дослідження бізнес-структурами для посилення захищеності переговорів у цифровому чи змішаному форматах. Рекомендації придатні для розробки корпоративних політик, навчальних програм та впровадження технологій захисту комерційної таємниці, репутації та конкурентних переваг.*
Ключові слова: *цифрова безпека, ділові переговори, кіберзагрози, інформаційна безпека, конфіденційність, кібергігієна, шифрування.*

DIGITAL SECURITY OF BUSINESS NEGOTIATIONS

Olena Bondarenko, PhD of Philosophy Sciences, associate professor, associate professor Department of Marketing and International Logistics, Odesa National Economic University, Odesa, Ukraine
e-mail: 7871996@gmail.com
ORCID: 0000-0001-9853-5051

Liliia Bondarenko, Teacher of Separate structural subdivision "Vocational College of Communication and Informatization" of the State University of Intelligent Technologies and Communication, Odesa, Ukraine
e-mail: liliiabondarenk@gmail.com
ORCID: 0009-0003-8984-5420

Abstract. *The aim of the article is to explore the phenomenon of digital security in business negotiations, to reveal its essence and importance for modern enterprises, to identify the most common threats in the digital environment, and to propose technological and organizational approaches that ensure confidentiality, integrity, and authenticity of sensitive information exchanged during negotiations. The study applies structural and logical analysis, comparison of international practices, and synthesis of scientific and analytical materials. The informational base includes academic literature, international information security standards (ISO/IEC 27001, ISO/IEC 27701), as well as reports, periodicals, and digital resources that reflect the current state of cybersecurity in business communication. The research has established that digital security of negotiations is a complex category that integrates technological (encrypted channels, VPN, DLP systems, multi-factor authentication), organizational (confidentiality policies, role-based access distribution, partner verification), and human (cyber hygiene, resistance to social engineering and phishing) dimensions. Key threats include unauthorized access to communication platforms (Zoom, Teams, Skype), data interception and theft, manipulation and disinformation, and phishing-based attacks. It is shown that a comprehensive system of measures significantly strengthens the resilience of negotiation processes to cyber risks and reduces the probability of data leakage. The findings can be applied by business entities to improve the protection of confidential information in online or hybrid negotiations. The recommendations may be used for drafting corporate information security strategies, implementing technical safeguards, and developing training programs for employees. This contributes to preventing financial losses, maintaining business reputation, and building long-term competitive advantages in the digital economy.*
Keywords: *digital security, business negotiations, cyber threats, information security, confidentiality, encryption, cyber hygiene.*

JEL Classification: M150; D830; M310

Постановка проблеми. У сучасному бізнес-просторі переговори стали ключовим елементом комунікацій, адже саме під час них узгоджуються умови співпраці, визначаються перспективи партнерства та ухвалюються стратегічні рішення. У цих процесах циркулює

чутлива інформація: фінансові звіти, умови угод, інноваційні ідеї та комерційні таємниці. Будь-який витік може зруйнувати репутацію компанії, знизити її конкурентоспроможність і спричинити значні фінансові втрати.

З поширенням цифрових технологій переговори дедалі частіше відбуваються у дистанційному форматі – через відеоконференції, корпоративні месенджери та онлайн-платформи. Це розширює можливості бізнесу, але водночас створює нові загрози: кібератаки, несанкціонований доступ і перехоплення даних. Тому формування надійної системи цифрової безпеки стає необхідною умовою захищеного обміну інформацією.

Важливим чинником ризику залишається людський фактор. Брак знань з кібергігієни, нехтування правилами безпеки чи вплив соціальної інженерії часто призводять до втрати даних. Це підкреслює необхідність поєднання технологічних рішень з організаційними заходами та підготовкою учасників переговорів, що сприяє формуванню корпоративної культури захищеності.

У глобалізованому середовищі безпека переговорів ускладнюється участю міжнародних партнерів, які діють у різних правових системах. Це вимагає уніфікації підходів до захисту даних і впровадження міжнародних стандартів, що зміцнюють довіру між сторонами.

Отже, дослідження спрямоване на систематизацію загроз цифровій безпеці ділових переговорів, оцінювання ефективності сучасних технологічних і організаційних інструментів та розробку практичних рекомендацій для бізнесу. Комплексні рішення, що поєднують технічний, правовий і психологічний підходи, є необхідною передумовою стійкості компаній у цифрову епоху.

Аналіз останніх досліджень і публікацій. Аналіз наукових праць останніх років засвідчує значний інтерес вітчизняних та зарубіжних дослідників до проблем цифрової та інформаційної безпеки. Водночас питання, пов'язані безпосередньо із забезпеченням цифрової безпеки ділових переговорів, залишаються недостатньо дослідженими.

Т. В. Бєльська, М. Г. Лашкіна та Ю. В. Нестеряк у статті «Інформаційна політика та інформаційна безпека держави як психосоціальне явище: проблеми та перспективи» [1] аналізують роль інформаційної політики у формуванні безпечного простору держави й суспільства. Інформаційна безпека трактується не лише технічно, а й у психосоціальному вимірі, з акцентом на вплив на свідомість, соціальну стабільність і державну безпеку. Визначаються загрози маніпуляції, дезінформації, інформаційних війн і кібератак. Автори підкреслюють потребу гармонізації національної політики з глобальними тенденціями та пропонують напрями її вдосконалення: підвищення інформаційної культури, зміцнення суверенітету й створення ефективних механізмів протидії сучасним загрозам.

В. С. Виздрик та О. М. Мельник у статті «Інформаційна безпека в Україні: сучасний стан» [3] досліджують стан захищеності інформаційного простору в умовах гібридних загроз і війни. Автори виокремлюють головні виклики – кібератаки, дезінформаційні кампанії, низьку цифрову грамотність та недоліки законодавства. Підкреслюється потреба у розвитку державної політики кіберзахисту, модернізації технічних засобів та міжнародній співпраці. Стаття робить акцент на комплексному підході, що поєднує правові, організаційні й технологічні інструменти.

В. О. Даніл'ян у статті «Інформаційна безпека в Україні: чинники та шляхи досягнення» [4] досліджує сучасний стан інформаційної безпеки, виокремлюючи ключові проблеми: зростання кіберзагроз, інформаційні війни, недосконале законодавство та потребу у розвитку національних інституцій. Автор підкреслює важливість стратегії, що включає вдосконалення нормативної бази, впровадження новітніх технологій, підвищення кіберграмотності й міжнародне співробітництво. Інформаційна безпека визначається як базова складова національної безпеки та фактор стабільності держави.

О. Дубровський у статті «Інформаційна безпека: суб'єктність і штучний інтелект» [5] досліджує роль ШІ у сфері безпеки. Автор розглядає питання суб'єктності ШІ, етичні та правові ризики його автономності й підкреслює потребу у взаємодії людини, організацій та інтелектуальних систем. Запропоновані концепції спрямовані на створення адаптивної системи захисту, що поєднує традиційні засоби кіберзахисту з можливостями ШІ.

В. Л. Кравчук у статті «Інформаційна безпека в контексті протидії чуткам» [6] аналізує вплив чуток на суспільну свідомість та їх використання у політичних і соціальних маніпуляціях. Розглядаються механізми поширення неправдивих повідомлень і небезпека для державної стабільності. Автор пропонує стратегії протидії: розвиток інформаційної політики, підвищення медіаграмотності та використання технологій перевірки інформації. Наголошується, що боротьба з чутками є складовою національної безпеки.

Н. М. Лисиця, О. О. Ястремська та О. Г. Вдовічена у статті «Стратегії ведення ділових переговорів в українському бізнес-середовищі» [7] досліджують специфіку переговорів в Україні. Автори аналізують підходи до їх ведення, враховуючи культурні, економічні й соціальні чинники, що формують бізнес-культуру. Окреслюються ефективні стратегії домовленостей, побудови довіри та уникнення конфліктів. Значну увагу приділено ролі психології, міжособистісної комунікації та етики. Подано практичні рекомендації щодо підвищення результативності переговорів та адаптації міжнародного досвіду до українських умов.

О. О. Носков та О. А. Дєгтяр у роботі «Інформаційна безпека України в умовах сучасних викликів» [8] аналізують основні загрози інформаційному простору держави – гібридні війни, кібератаки, поширення дезінформації та маніпуляції громадською свідомістю. Автори наголошують на ролі державної політики, міжнародного співробітництва й правової бази, на необхідності комплексного поєднання технічних, правових і організаційних заходів.

О. І. Пугачов у праці «Інформаційна безпека в умовах розвитку глобалізованого світу» [9] розглядає загрози, зумовлені глобалізацією, цифровізацією та зростанням кіберзалежності. Акцент зроблено на міжнародній співпраці, вдосконаленні нормативної бази та розвитку технологій захисту. Автор підкреслює, що інформаційна безпека визначає стабільність держави, конкурентоспроможність бізнесу та захист прав громадян. Запропоновано комплексний підхід, який включає технічні, організаційні та освітні заходи для мінімізації ризиків і формування культури безпечного використання даних.

У монографії «Корпоративна інформаційна безпека» В. І. Чубаєвський [10] аналізує теоретичні й практичні засади захисту корпоративних інформаційних ресурсів. Розглянуто правові, технічні та організаційні механізми протидії кіберзагрозам, управління ризиками, міжнародні стандарти й інструменти їх впровадження у діяльність підприємств. Монографія спрямована на побудову комплексної системи корпоративної інформаційної безпеки.

Л. В. Шостак, О. О. Помазун та А. А. Федонюк у статтях «Інформаційно-цифрова безпека електронної торгівлі» [11] та «Інформаційна безпека в контексті інноваційного розвитку бізнес-моделі вітчизняних підприємств в умовах цифрової економіки» [12] визначають інформаційну безпеку як ключовий чинник цифрової економіки. Вони аналізують вплив кіберзагроз на інноваційні бізнес-моделі та доводять, що конкурентоспроможність і стійкість підприємств залежать від інтеграції захисту даних у бізнес-процеси.

Н. В. Шульженко у статті «Інформаційна безпека суспільства від загроз організованої злочинності» [13] досліджує використання транснаціональними злочинними угрупованнями цифрових технологій для кіберзлочинів, фінансових махінацій та впливу на суспільні процеси. Аналізуються загрози критичній інфраструктурі, державним інституціям і громадянам, підкреслюється потреба вдосконалення національних і міжнародних механізмів протидії. Авторка пропонує стратегію, що поєднує правові, організаційні й технічні заходи.

А. І. Ясінська у статті «Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації» [14] розглядає формування системи корпоративної безпеки, основні загрози та принципи захисту даних. Авторка акцентує на конфіденційності, цілісності та доступності інформації, підкреслюючи, що стратегія безпеки має поєднувати технічні рішення, корпоративну культуру, навчання персоналу та міжнародні стандарти.

Відокремлення невирішених раніше частин загальної проблеми. Попри значний науковий та практичний інтерес до проблематики цифрової безпеки, низка аспектів ділових переговорів залишається недостатньо опрацьованою. Сучасні дослідження здебільшого зосереджені на технічних рішеннях – захищених каналах комунікацій, шифруванні чи інструментах автентифікації. Водночас менш уваги приділяється організаційним і психологічним чинникам, які безпосередньо впливають на стійкість бізнес-процесів.

Зокрема, актуальним є питання взаємодії між технічними й управлінськими підходами до забезпечення конфіденційності. Бракує системних досліджень, що пояснюють, як поєднання політик безпеки, корпоративної культури та цифрових технологій здатне створити комплексний захист переговорів. Недостатньо розроблені також підходи до оцінювання рівня кібергігієни персоналу та впливу людського фактора на загальну ефективність системи безпеки.

Окремої уваги потребує міжнародний контекст. Учасники переговорів нерідко діють у різних правових системах і керуються різними стандартами цифрової безпеки. Це ускладнює гармонізацію вимог та створює додаткові ризики під час обміну конфіденційними даними. На практиці це означає, що без уніфікації правил та впровадження міжнародних стандартів компанії залишаються вразливими до витоку інформації.

Отже, дослідження цифрової безпеки ділових переговорів має орієнтуватися не лише на технологічний вимір, а й на організаційні та правові аспекти. Усунення цих прогалин дозволить сформувати більш цілісне уявлення про природу ризиків і забезпечити практичні рекомендації для бізнесу.

Мета дослідження полягає у всебічному аналізі проблем і викликів, пов'язаних із забезпеченням цифрової безпеки ділових переговорів, а також у визначенні ефективних підходів до їх захисту. Дослідження спрямоване на виявлення ризиків цифрового середовища, розкриття можливостей застосування правових та технологічних інструментів, а також обґрунтування значення формування корпоративної культури безпеки як невід'ємного чинника підвищення рівня захищеності переговорних процесів у сучасному бізнес-середовищі.

Основний матеріал. Цифрова безпека переговорів – це комплекс заходів технічного, організаційного та правового характеру, спрямованих на забезпечення конфіденційності, цілісності та автентичності інформації, яка використовується під час комунікацій у цифровому середовищі. Її сутність полягає в тому, щоб гарантувати надійний захист від несанкціонованого доступу, запобігати витоку даних і створювати умови для безпечної взаємодії між сторонами, які ведуть переговори. У сучасному бізнесі цифрова безпека є не лише технічним інструментом, а й ключовим чинником довіри між партнерами, що визначає перспективи подальшої співпраці.

Особливості ділових переговорів у цифровому середовищі пов'язані з використанням онлайн-інструментів – відеоконференцій, електронної пошти, корпоративних месенджерів та хмарних платформ для обміну документами.

З одного боку, ці технології підвищують ефективність комунікації, скорочують витрати часу та ресурсів, забезпечують гнучкість у виборі формату взаємодії.

З іншого боку, вони створюють додаткові ризики, адже цифровий простір відкриває доступ до стратегічної інформації для потенційних зловмисників. Тому успішність переговорів дедалі більше залежить від здатності сторін інтегрувати технологічні рішення, що мінімізують загрози та забезпечують контрольованість процесу.

Серед основних загроз цифровій безпеці переговорів виділяють декілька ключових напрямів. По-перше, це кіберзлочинність, яка проявляється у вигляді атак хакерів на комунікаційні канали чи сервери компаній з метою перехоплення даних або їх блокування.

По-друге, фішинг, що ґрунтується на психологічних маніпуляціях і спрямований на отримання конфіденційної інформації шляхом підробки електронних листів чи вебресурсів. По-третє, витік даних, який може бути як наслідком зовнішнього втручання, так і результатом людських помилок або недбалості співробітників. Усі ці фактори становлять серйозну небезпеку для результативності переговорів, адже компрометація стратегічної інформації здатна підірвати позиції компанії на ринку та завдати довгострокових збитків.

Отже, цифрова безпека переговорів є багатогранним явищем, що поєднує технічні, організаційні та соціальні аспекти. Її ефективне забезпечення вимагає комплексного підходу, який охоплює як захист інформаційних систем і каналів зв'язку, так і формування культури безпечної поведінки учасників переговорів (табл. 1).

Таблиця 1

Основні загрози цифровій безпеці переговорів та їх наслідки для бізнесу

Загроза	*Сутність*	*Можливі наслідки для бізнесу*
Кіберзлочинність	Хакерські атаки на канали комунікації, сервери чи хмарні сервіси	Викрадення стратегічних даних, блокування переговорів, фінансові втрати
Фішинг	Використання підроблених листів, сайтів або повідомлень для виманювання даних	Компрометація акаунтів, отримання доступу до конфіденційної інформації, зниження довіри партнерів
Витік даних	Несанкціонований доступ до документів через зовнішні атаки чи помилки персоналу	Втрата конкурентних переваг, репутаційні ризики, юридична відповідальність
Соціальна інженерія	Маніпуляції учасниками переговорів для отримання чутливої інформації	Розкриття комерційних таємниць, підрив позицій у переговорах

Недостатній захист ІТ	Використання незахищених месенджерів, відсутність шифрування даних	Перехоплення переговорів у реальному часі, підробка документів

Джерело: складено авторами на основі [2, 11, 12, 15]

Сучасні ділові переговори дедалі частіше проходять у цифровому середовищі, що значно розширює можливості комунікації, але водночас створює нові виклики у сфері безпеки. Одним із ключових ризиків є несанкціонований доступ до каналів зв'язку, таких як Zoom, Microsoft Teams, Skype чи інші онлайн-платформи. Використання недостатньо захищених паролів, відсутність багатофакторної автентифікації або недотримання правил кібергігієни може дозволити зловмисникам підключитися до зустрічі та отримати доступ до конфіденційних матеріалів. Відомі випадки так званого «zoom-bombing» свідчать, що навіть випадкове втручання сторонніх осіб здатне зірвати переговори та підірвати довіру між учасниками.

Не менш серйозною загрозою є викрадення та перехоплення даних. Інформація, що передається під час переговорів, може бути перехоплена хакерами через атаки «людина посередині» (MITM), шкідливе програмне забезпечення чи незахищені канали передачі. У результаті зловмисники отримують доступ до стратегічних планів компаній, умов контрактів або фінансових показників. Такі дані можуть бути використані для недобросовісної конкуренції, шантажу або продажу третім особам.

Окрему небезпеку становлять маніпуляції з інформацією та дезінформація. Зловмисники можуть змінювати зміст переданих документів, поширювати неправдиві повідомлення від імені офіційних учасників або створювати підроблені протоколи переговорів. Такі дії підривають достовірність комунікації та можуть призвести до прийняття неправильних рішень, що шкодять бізнесу. У міжнародних переговорах дезінформація особливо небезпечна, адже вона може впливати не лише на репутацію компанії, а й на міждержавні відносини (табл. 2).

Таблиця 2

Основні загрози цифровій безпеці переговорів

Загроза	*Механізм реалізації*	*Можливі наслідки*
Несанкціонований доступ до каналів зв'язку (Zoom, Teams, Skype)	Використання слабких паролів, відсутність MFA, «zoom-bombing»	Зрив переговорів, витік конфіденційних матеріалів, підрив довіри
Викрадення та перехоплення даних	Атаки «людина посередині» (MITM), шкідливе ПЗ, незахищені канали	Доступ до стратегічних планів, умов контрактів, фінансових даних; шантаж або конкурентні переваги зловмисників
Маніпуляції з інформацією та дезінформація	Підробка документів, фальшиві повідомлення, модифікація переданих даних	Прийняття хибних рішень, втрати бізнесу, шкода репутації, ускладнення міжнародної співпраці
Соціальна інженерія та фішинг	Підроблені листи з посиланнями/вкладеннями, телефонне шахрайство, психологічний тиск	Витік даних ще до початку переговорів, зараження систем, несанкціонований доступ до корпоративних ресурсів

Джерело: складено авторами на основі [2, 11, 12, 15]

Ще однією поширеною загрозою є соціальна інженерія та фішингові атаки на учасників переговорів. Хакери активно використовують людський фактор як найслабшу ланку інформаційної безпеки. Учасникам надсилають електронні листи з підробленими посиланнями на платформи для переговорів чи вкладеннями, що містять шкідливе програмне забезпечення. Крім того, поширеним є метод телефонного шахрайства, коли зловмисники представляються технічними спеціалістами й переконують надати доступ до корпоративних систем. Подібні атаки здатні призвести до витоку критично важливої інформації ще до початку переговорів.

Отже, цифрова безпека переговорів перебуває під постійним тиском широкого спектра загроз. Для їх нейтралізації компаніям необхідно впроваджувати комплексні заходи захисту, поєднуючи сучасні технології шифрування з підвищенням обізнаності персоналу та розробкою чітких регламентів безпечної поведінки під час переговорів.

Забезпечення цифрової безпеки переговорів неможливе без застосування сучасних технічних рішень, спрямованих на захист інформації від несанкціонованого доступу, витоків та кібератак. Технологічні інструменти виконують ключову роль у створенні безпечного середовища комунікацій, де зберігаються конфіденційність, цілісність і доступність даних.

Використання шифрованих каналів зв'язку. Захищені комунікаційні протоколи (TLS, SRTP, E2EE) дозволяють унеможливити перехоплення інформації під час онлайн-переговорів у платформах Zoom, Microsoft Teams чи Skype. Завдяки наскрізному шифруванню дані доступні лише безпосереднім учасникам переговорів, що істотно знижує ризики втручання третіх сторін.

Двофакторна аутентифікація та управління доступом. Багаторівневі методи ідентифікації (пароль + SMS-код або застосунок-аутентифікатор) створюють додатковий бар'єр для зловмисників. Управління доступом на основі ролей дозволяє чітко розмежувати права учасників переговорів, мінімізуючи ризики витоку конфіденційної інформації через внутрішні загрози (табл. 3).

Таблиця 3

Інструменти цифрової безпеки переговорів

Інструмент / технологія	*Призначення*	*Переваги*	*Обмеження*
Шифровані канали зв'язку (TLS, E2EE, SRTP)	Захист аудіо-, відео- та текстових даних від перехоплення	- Високий рівень конфіденційності - Недоступність даних для третіх осіб	- Залежність від якості реалізації у сервісах (Zoom, Teams) - Може знижувати швидкість передачі даних
Двофакторна аутентифікація (2FA)	Контроль доступу до переговорних платформ та документів	- Суттєво підвищує безпеку входу - Простота впровадження	- Може ускладнити користування - Ризик втрати доступу при відсутності другого фактору
Управління доступом (RBAC, ABAC)	Розмежування прав користувачів відповідно до ролей	- Мінімізує внутрішні загрози - Гнучкість у налаштуванні доступу	- Необхідність постійного адміністрування - Ризик людських помилок при налаштуванні
Системи DLP (Data Loss Prevention)	Запобігання витоку конфіденційних документів	- Виявлення та блокування підозрілих дій - Централізований контроль над файлами	- Висока вартість впровадження - Потреба у налаштуванні під специфіку бізнесу
VPN (Virtual Private Network)	Створення захищеного з'єднання між учасниками переговорів	- Приховує трафік від атак - Захищає при роботі у публічних мережах	- Залежність від якості сервера VPN - Може знижувати швидкість інтернет-з'єднання
Захищені сервери (сертифіковані, ISO/IEC 27001)	Розміщення даних і комунікацій у безпечному середовищі	- Відповідність міжнародним стандартам - Підвищення довіри партнерів	- Вартість обслуговування - Необхідність постійного моніторингу безпеки

Джерело: складено авторами на основі [2, 11, 12, 15]

Системи контролю конфіденційних документів (DLP). Технології Data Loss Prevention забезпечують моніторинг, виявлення та блокування спроб несанкціонованого копіювання чи пересилання важливих файлів. Використання DLP-систем під час переговорів дає можливість зберігати контроль над документами навіть у випадку роботи у дистанційному форматі.

Використання VPN та захищених серверів. Віртуальні приватні мережі гарантують захищене з'єднання між учасниками переговорів, приховуючи трафік від потенційних атак. Розміщення даних і комунікаційних процесів на захищених серверах, що відповідають міжнародним стандартам інформаційної безпеки, забезпечує додатковий рівень надійності та підвищує довіру між сторонами.

Застосування сучасних технологій дозволяє бізнесу не лише зменшувати ризики витоку критично важливої інформації, а й формувати довгострокову культуру безпеки. Поєднання технічних засобів та організаційних заходів створює цілісну систему захисту, необхідну для успішних і безпечних переговорів у цифрову епоху.

Забезпечення безпеки неможливе лише технологіями. Вирішальну роль відіграють організаційні заходи, що регламентують правила і процедури, спрямовані на мінімізацію ризиків витоку та зловживань. Саме поєднання технічних рішень та управлінських підходів формує комплексний захист ділових комунікацій.

Ключовим кроком є політика конфіденційності, яка визначає порядок підготовки, проведення та збереження даних переговорів, регламентує використання цифрових платформ і відповідальність за розголошення. Важливим доповненням є розмежування доступу: різні групи учасників отримують різні права – від повного доступу до ознайомчого перегляду, що знижує ризики несанкціонованого використання інформації.

Значну роль відіграє навчання працівників кібергігієні. Практика доводить: навіть найсучасніші рішення втрачають ефективність за низької обізнаності персоналу. Регулярні тренінги з протидії фішингу та роботи із захищеними каналами формують корпоративну культуру безпечного користування цифровими інструментами.

Необхідною умовою є також перевірка партнерів і контрагентів.

У глобалізованому середовищі вона дає змогу уникнути співпраці з ненадійними організаціями, що мають слабкі системи захисту чи приховані інтереси. Аудит надійності, перевірка репутації та оцінка політик безпеки допомагають знизити ризики співпраці.

Отже, організаційні заходи безпеки є невід'ємним доповненням технічних інструментів: вони забезпечують системність, підвищують дисципліну та формують довіру між сторонами – ключову умову успішних переговорів у цифрову епоху.

Висновки. У сучасному бізнес-середовищі цифрова безпека переговорів є стратегічним чинником успіху компаній. Переговори – це не лише інструмент домовленостей, а й процес обміну чутливою інформацією: фінансовими даними, умовами контрактів, інноваціями та комерційними таємницями. Витік таких відомостей може спричинити економічні збитки, втрату довіри та конкурентних переваг.

Цифрова безпека переговорів охоплює заходи для збереження конфіденційності, цілісності та доступності даних. Поширення онлайн- та гібридних форматів комунікації створює додаткові ризики, пов'язані з використанням електронних платформ і глобальних каналів зв'язку.

Серед основних загроз виокремлюються: несанкціонований доступ до комунікацій, перехоплення та викрадення даних, маніпуляції, дезінформація, а також соціальна інженерія та фішинг. Для їх нейтралізації потрібне поєднання технічних і організаційних рішень.

Технічні інструменти – шифрування, двофакторна аутентифікація, VPN, захищені сервери – значно знижують ризики, проте ефективність забезпечується лише за умови належної організації процесів. Важливими є й організаційні заходи: політика конфіденційності, розмежування доступу, навчання персоналу кібергігієні та перевірка партнерів. Саме вони мінімізують людський фактор як головне джерело вразливостей.

Отже, цифрова безпека переговорів – це багатовимірна система, що інтегрує технічні, організаційні та психологічні аспекти. Лише комплексний підхід гарантує захист стратегічної інформації, зміцнює довіру між сторонами й забезпечує стійкість бізнесу. Подальші дослідження мають бути спрямовані на розробку універсальних стандартів і практик, адаптованих до міжнародного контексту та динаміки технологій.

Список літератури

1. Бєльська Т., Лашкіна М., Нестеряк Ю. Інформаційна політика та інформаційна безпека держави як психосоціальне явище: проблеми та перспективи. *Публічне управління.* 2020. № 22 (2). С. 119–132. DOI: https://doi.org/10.32689/2617-2224-2020-2(22)-119-132
2. Бондаренко О. М., Бондаренко, Л. Г. Цифрові комунікації в ділових переговорах. *Бізнес Інформ.* 2025. № 1(564). С. 517–531. DOI: https://doi.org/10.32983/2222-4459-2025-1-517-531
3. Виздрик В. С., Мельник О. М. Інформаційна безпека в Україні: сучасний стан. *Грааль науки.* 2023. №24. С. 196–202. DOI: https://doi.org/ 10.36074/grail-of-science.17.02.2023.034
4. Даніл'ян В. Інформаційна безпека в Україні: чинники та шляхи досягнення. *Theoretical and practical aspects of modern scientific research. Sociology and statistics*. 2021. № 24. С. 10-12. DOI: https://doi.org/10.36074/logos-30.04.2021.v2.01
5. Дубовський О. Інформаційна безпека: суб'єктність і штучний інтелект. *Journal of Innovations and Sustainability.* 2024. № 8(2). 09. DOI: https://doi.org/10.51599/is.2024.08.02.09
6. Кравчук В. Л. Інформаційна безпека в контексті протидії чуткам. *Європейські перспективи.* 2024. № 4. С. 260–264. DOI: https://doi.org/ 10.71404/ep.2024.4.36
7. Лисиця Н. М., Ястремська О. О., Вдовичена О. Г. Стратегії ведення ділових переговорів в українському бізнес-середовищі. *Актуальні питання у сучасній науці.* 2023. № 9(15). С. 74-82. DOI: https://doi.org/10.52058/2786-6300-2023-9(15)-74-82
8. Носков О., Дєгтяр О. Інформаційна безпека України в умовах сучасних викликів. *Національні інтереси України.* 2025. № 6(11). С. 147–158. DOI: https://doi.org/10.52058/3041-1793-2025-6(11)-147-158
9. Пугачов О. І. Інформаційна безпека в умовах розвитку глобалізованого світу. *Суспільство та національні інтереси*. 2024. 5(5). С. 627–639. DOI: https://doi.org/10.52058/3041-1572-2024-5(5)-627-639
10. Чубаєвський В. І. Корпоративна інформаційна безпека : монографія. Київ : Держ. торг.-екон. ун-т, 2022. 272 с. DOI: https://doi.org/10.31617/ m.knute.2022-242
11. Шостак Л. В., Федонюк А. А., Помазун О. О. Інформаційно-цифрова безпека електронної торгівлі. *Цифрова економіка та економічна безпека.* 2025. №2 (17), С. 219–223. DOI: https://doi.org/10.32782/dees.17-36
12. Шостак Л. В., Помазун О. О. Інформаційна безпека в контексті інноваційного розвитку бізнес-моделі вітчизняних підприємств в умовах цифрової економіки. *Цифрова економіка та економічна безпека.* 2024. №5 (14). С. 160–165. DOI: https://doi.org/10.32782/dees.14-25
13. Шульженко Н. В. Інформаційна безпека суспільства від загроз організованої злочинності. *Наукові Перспективи (Naukovì Perspektivi)*. 2023. №12(30). С. 367–373. DOI: https://doi.org/10.52058/2708-7530-2022-12(30)-367-373
14. Ясінська А. І. Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації. *Економіка та суспільство.* 2023. №56. DOI: https://doi.org/10.32782/2524-0072/2023-56-118
15. Seaman J. Cyber Security and the Digital Business. *Protective Security.* 2021. P. 213–269. DOI: https://doi.org/10.1007/978-1-4842-6908-4_6

References

1. Bielska, T., Lashkina, M., & Nesteriak, Yu. (2020). Information policy and information security of the state as a psychosocial phenomenon: problems and prospects. *Publichne upravlinnia*, 22 (2), 119–132. DOI: https://doi.org/ 10.32689/2617-2224-2020-2(22)-119-132 [In Ukrainian].
2. Bondarenko, O. M., & Bondarenko, L. H. (2025). Digital Communications in Business News. *Biznes Inform*, 1(564), 517–531. DOI: https://doi.org/ 10.32983/2222-4459-2025-1-517-531 [In Ukrainian].
3. Vizdryk, V., & Melnyk, O. (2023). Information security in Ukraine: current situation. *Hraal nauky*, 24, 196–202. DOI: https://doi.org/10.36074/grail-of-science.17.02.2023.034 [In Ukrainian].
4. Danilian, V. (2021). Information security in Ukraine: origins and ways to achieve it *Teoretychni ta praktychni aspekty suchasnykh naukovykh doslidzhen*. 24. 10-12. DOI: https://doi.org/10.36074/logos-30.04.2021.v2.01 [In Ukrainian].

5. Dubovskyi, O. (2024). Information security: subjectivity and artificial intelligence. *Journal of Innovations and Sustainability*, 8(2), 09. DOI: https://doi.org/ 10.51599/is.2024.08.02.09 [In Ukrainian].
6. Kravchuk, V. L. (2024). Information security in the context of the current crisis. *Yevropeiski perspektyvy,* 4. 260–264. DOI: https://doi.org/10.71404/ ep.2024.4.36 [In Ukrainian].
7. Lysytsia, N., Yastremska, O., & Vdovychena, O. (2023). Strategies for conducting business negotiations in the Ukrainian business environment. *Aktualni Pytannia u Suchasnii Nautsi,* 9(15), 74-82. DOI: https://doi.org/10.52058/2786-6300-2023-9(15)-74-82 [In Ukrainian].
8. Noskov, O., & Diehtiar, O. (2025). Information security of Ukraine in the conditions of current crises. *Natsionalni Interesy Ukrainy*, 6(11). 147–158. DOI: https://doi.org/10.52058/3041-1793-2025-6(11)-147-158 [In Ukrainian].
9. Puhachov, O. (2024). Information security in the conditions of the development of the globalized world.. *Suspilstvo ta Natsionalni Interesy,* 5(5). 627–639. DOI: https://doi.org/10.52058/3041-1572-2024-5(5)-627-639 [In Ukrainian].
10. Chubaievskyi, V. I. (2022). Korporatyvna informatsiina bezpeka. DOI: https://doi.org/10.31617/m.knute.2022-242 [In Ukrainian].
11. Shostak, L. V., Fedoniuk, A. A., Pomazun O. O. (2025). Information and digital security of electronic commerce. *Tsyfrova Ekonomika ta Ekonomichna Bezpeka*, 2 (17), 219–223. DOI: https://doi.org/10.32782/dees.17-36 [In Ukrainian].
12. Shostak, L. V., & Pomazun, O. O. (2024). Information security in the context of innovative development of business models of domestic enterprises in the conditions of the digital economy. *Tsyfrova Ekonomika ta Ekonomichna Bezpeka*, 5 (14), 160–165. DOI: https://doi.org/10.32782/dees.14-25 [In Ukrainian].
13. Shulzhenko, N. (2023). Information security of society as a threat of organized crime. *Naukovi Perspektyvy (Naukovì Perspektivi)*, 12(30). 367–373. DOI: https://doi.org/10.52058/2708-7530-2022-12(30)-367-373 [In Ukrainian].
14. Iasinska, A. (2023). Information security of an enterprise: conceptual principles of effective information security. *Ekonomika ta Suspilstvo*, 56. DOI: https://doi.org/10.32782/2524-0072/2023-56-118 [In Ukrainian].
15. Seaman, J. (2021). Cyber Security and the Digital Business. *Protective Security*, 213–269. DOI: https://doi.org/10.1007/978-1-4842-6908-4_6

Стаття надійшла до редакції 12.08.2025
Прийнята до публікації 25.08.2025
Опубліковано онлайн 25.09.2025