DOI: 10.15276/EJ.01.2025.14
DOI: 10.5281/zenodo.18025510
UDC: 658.012.4:004.7
JEL: M15, L86, D81

ФОРМУВАННЯ ІНФОКОМУНІКАЦІЙНОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА В УМОВАХ КРИЗ

FORMATION OF AN ENTERPRISE'S INFORMATION AND COMMUNICATION INFRASTRUCTURE IN CRISIS CONDITIONS

Ali Rashed Khalifa Bumeqairaa Almansoori
Odesa Polytechnic National University, Odesa, Ukraine
ORCID: 0009-0005-1875-4884

Received 29.02.2025

Алі Рашид Халіфа Бумекайр Альмансурі. Формування інфокомунікаційної інфраструктури підприємства в умовах криз. Науково-методична стаття.
Стаття присвячена формуванню інфокомунікаційної інфраструктури підприємства в умовах криз. Визначено структуру інфокомунікаційних систем, що включає архітектуру технічних, мережевих, хмарних та програмних рішень, а також інтегрованих цифрових середовищ, які забезпечують безперебійний рух інформаційних потоків, оперативність взаємодії та доступність даних для управлінських рішень. Досліджено ризики і вразливості цифрової інфраструктури, зумовлені впливом зовнішніх кризових факторів, кібератак, технічних збоїв, дефіциту людського капіталу цифрових компетенцій та зростаючою залежністю підприємства від інформаційно-комунікаційних платформ та провайдерів цифрових послуг. Проаналізовано функції інфокомунікаційних ресурсів у запобіганні та подоланні кризових явищ, що проявляються у забезпеченні координації між підрозділами, підтримці прозорості процесів, швидкому поширенні даних, підвищенні точності управлінських рішень та посиленні цифрової стійкості підприємства.
Ключові слова: інфокомунікації, інфокомунікаційна інфраструктура, підприємство, криза, система, цифровізація, функції, ризики

Ali Rashed Khalifa Bumeqairaa Almansoori. Formation of an Enterprise's Information and Communication Infrastructure in Crisis Conditions. Scientific and methodical article.
The article is devoted to the formation of an enterprise's information and communication infrastructure in crisis conditions. The structure of information and communication systems is defined, including the architecture of technical, network, cloud and software solutions, as well as integrated digital environments that ensure the uninterrupted flow of information, prompt interaction and the availability of data for management decisions. The risks and vulnerabilities of digital infrastructure caused by external crisis factors, cyberattacks, technical failures, a shortage of human capital with digital competencies, and the growing dependence of enterprises on information and communication platforms and digital service providers are examined. The functions of information and communication resources in preventing and overcoming crisis phenomena are analysed, which manifest themselves in ensuring coordination between departments, maintaining transparency of processes, rapid dissemination of data, increasing the accuracy of management decisions and strengthening the digital resilience of the enterprise.
Keywords: infocommunications, infocommunications infrastructure, enterprise, crisis, system, digitalisation, functions, risks

Сучасні умови функціонування підприємств характеризуються високим рівнем невизначеності, зростанням системних ризиків та посиленням кризових явищ, зумовлених глобальними економічними дисбалансами, цифровою трансформацією та зовнішніми шоками. За таких обставин особливої актуальності набуває питання формування інфокомунікаційної інфраструктури підприємства як базового елементу забезпечення безперервності діяльності, адаптивності управлінських рішень та стійкості бізнес-процесів. Інфокомунікаційна інфраструктура виступає інтегруючою основою для обробки, передачі та використання інформаційних ресурсів підприємства, забезпечуючи взаємозв'язок між управлінськими, виробничими та комунікаційними підсистемами. В умовах кризи її роль суттєво зростає, оскільки саме цифрові та інформаційно-комунікаційні рішення дозволяють оперативно реагувати на зміни зовнішнього середовища, мінімізувати втрати, підтримувати керованість організаційних структур і зберігати конкурентоспроможність. Попри наявність значної кількості наукових досліджень, присвячених цифровізації та інформаційним технологіям у діяльності підприємств, питання цілісного формування інфокомунікаційної інфраструктури з урахуванням кризових умов залишається недостатньо систематизованим. Більшість існуючих підходів орієнтовані на стабільні умови розвитку та не повною мірою враховують обмеженість ресурсів, зростання ризиків і потребу в підвищенні організаційної гнучкості У зв'язку з цим дослідження проблематики формування інфокомунікаційної інфраструктури підприємства в умовах кризи є своєчасним і науково обґрунтованим. Воно спрямоване на поглиблення теоретичних положень і розвиток практичних підходів до забезпечення стійкого функціонування підприємств шляхом ефективного використання інфокомунікаційних ресурсів та технологій в умовах кризових викликів.

Метою статті є обґрунтування теоретичних положень і розроблення науково-практичних підходів до формування інфокомунікаційної інфраструктури підприємства в умовах кризи з метою підвищення стійкості його функціонування, адаптивності системи управління та ефективності бізнес-процесів в умовах зростання невизначеності й ризиків. Для її досягнення варто виконати такі завдання:

а) визначити структуру інфокомунікаційних систем;

б) дослідити ризики і вразливості цифрової інфраструктури;

в) проаналізувати функції інфокомунікаційних ресурсів у запобіганні та подоланні кризових явищ.

Роль інфокомунікаційних систем полягає у забезпеченні цілісного інформаційно-комунікаційного простору, який дає змогу підприємству підтримувати узгодженість операцій та стабільність управлінських процесів навіть у ситуаціях криз. Завдяки цій інфраструктурній основі відбувається оперативна передача критично важливих даних, своєчасна координація дій між підрозділами та збереження доступності інформаційних ресурсів, що є ключовими умовами ефективного реагування на кризові впливи. Структура інфокомунікаційних ресурсів містить такі структурні елементи: інформаційні, інфраструктурні, технологічні, комунікаційні ресурси та ресурси цифрової безпеки. Однак для цілісного розуміння їх ролі у забезпеченні стійкого функціонування підприємства недостатньо лише ідентифікувати наявні цифрові активи. Важливо простежити, яким чином ці ресурси інтегруються між собою, взаємодіють у межах єдиного інформаційного простору та утворюють комплексну інфокомунікаційну систему, що забезпечує узгоджені інформаційні потоки, оперативний обмін даними та підтримку управлінських процесів.

Аналіз останніх досліджень і публікацій

У сучасних умовах цифрової трансформації інфокомунікаційні системи підприємства сформувалися як комплексна архітектура, що охоплює інформаційні, технологічні, комунікаційні та безпекові компоненти, інтегровані в єдиний управлінський простір. Зарубіжні дослідження підтверджують, що ефективність взаємодії цих елементів визначає рівень адаптивності підприємства, його операційну узгодженість та здатність забезпечувати стійкість у мінливих умовах.

Значущу роль інформаційної складової підтверджує дослідження [1], у якому обґрунтовано, що управлінські інформаційні системи забезпечують формування своєчасних, релевантних та аналітично цінних даних, необхідних для прийняття ефективних рішень. Це безпосередньо стосується інформаційного елемента інфокомунікаційної системи, який формує інформаційні потоки, підтримує аналітичну діяльність і забезпечує прозорість бізнес-процесів. Подібні результати отримано у дослідженні [2], де підкреслено, що якість даних, їхня доступність та інтеграція визначають швидкість операцій, гнучкість управління й рівень внутрішньої координації. Це демонструє критичність інформаційних ресурсів як основу функціонування всієї системи. Класичний висновок автора [3], який розробив модель детермінант ефективності організаційних інформаційних систем, також належить до інформаційного елемента інфокомунікаційної системи, оскільки описує залежність організаційних результатів від структури, форми та якості інформації, що циркулює в системі.

Дослідження [4] показує, що ERP-системи підсилюють внутрішню та зовнішню інтеграцію, оптимізують ланцюги постачання та підвищують ефективність операцій. ERP виступає основою технологічного елемента інфокомунікаційної системи, забезпечуючи стандартизацію процесів, централізацію даних та інтеграцію з цифровими системами підприємства. Аналогічно з попереднім дослідженням, результати [5] свідчать про суттєве зростання фінансових результатів підприємств, що впровадили ERP. Це підтверджує, що технологічний елемент інфокомунікаційної системи є ключовим джерелом підвищення ефективності операцій і конкурентоспроможності. Суттєвий інституційний аспект технологічної складової аналізує [6], доводячи, що цінність корпоративних інформаційних систем залежить від ефективності корпоративного управління. Це стосується стратегічно-управлінського рівня інфокомунікаційного середовища, де технологічні рішення поєднуються з організаційними механізмами.

Комунікаційна складова інфокомунікаційної системи визначає, наскільки ефективно підприємство організовує внутрішню та зовнішню взаємодію. У дослідженнях інформаційних систем NASA, виконаних [7], показано, що інфокомунікаційна система може виконувати функції забезпечення стабільності операцій, узгодження даних та мінімізацію впливів криз у періоди організаційних змін. Це безпосередньо демонструє роль комунікаційних інструментів у підтримці стійкості.

Робота [8] підкреслює тенденцію до переходу від традиційних інформаційних систем до інтелектуальних, що включають експертні модулі, засоби підтримки рішень і знаннєві технології. Цей напрям є ключовим для інтеграційно-аналітичного елемента інфокомунікаційної системи, оскільки демонструє, як системи синхронізують інформацію та забезпечують адаптивність у складних управлінських ситуаціях. В свою чергу модель [9], яка описує еволюцію інформаційних систем від підсистем обліку до стратегічно орієнтованих цифрових платформ, також належить до цього елемента. Вона демонструє, як відбувається поступове нарощування інтеграції, масштабування та розширення функціональності інфокомунікаційної системи відповідно до потреб підприємства.

Науковці [10] досліджують роль ERP у забезпеченні точності, цілісності та доступності облікової інформації. Їх висновки прямо стосуються елемента цифрової безпеки інфокомунікаційної системи, оскільки ERP виступає основою захисту даних, зниження ризиків помилок і забезпечення відповідності регуляторним вимогам. В свою чергу [7] також частково торкається питання операційної стійкості, доводячи, що інфокомунікаційна система здатна виступати «амортизатором криз» у періоди структурних змін, що є ключовим для розуміння ролі безпекового та стійкісного елементів інфокомунікаційної системи.

Виклад основного матеріалу дослідження

В той же час важливим є інтеграційно-аналітичний елемент, який не входить до переліку інфокомунікаційних ресурсів підприємства, оскільки не є окремим видом цифрового активу. Але його інтеграція є важливою, адже на рівні функціонування інфокомунікаційної системи необхідний окремий комплекс механізмів, що забезпечують узгодження, аналітичну обробку даних та синхронізація інформаційних потоків.

Тим самим проведений аналіз зарубіжних джерел підтверджує, що інфокомунікаційна система підприємства виступає багатовимірною архітектурою, де:

— інформаційний елемент забезпечує якість, доступність і релевантність даних;
— технологічно-інфраструктурний елемент формує цифровий фундамент операцій;
— комунікаційний елемент забезпечує інтегровану взаємодію і координацію;
— інтеграційно-аналітичний елемент створює можливості для інтелектуалізації та адаптивності;
— елемент цифрової безпеки та стійкості гарантує надійність і захищеність функціонування системи.

Такий підхід дозволяє розглядати інфокомунікаційну систему підприємства не як набір окремих цифрових інструментів, а як цілісну архітектуру, що забезпечує стале функціонування підприємства та його здатність реагувати на кризові виклики. Взаємодія інформаційних, технологічних, комунікаційних та безпекових компонентів формує підґрунтя для безперервності бізнес-процесів і швидкого переналаштування інформаційних потоків у нестабільних умовах. Розглянемо структуру інфокомунікаційної системи підприємства, що функціонує під впливом зовнішніх криз (рис. 1).

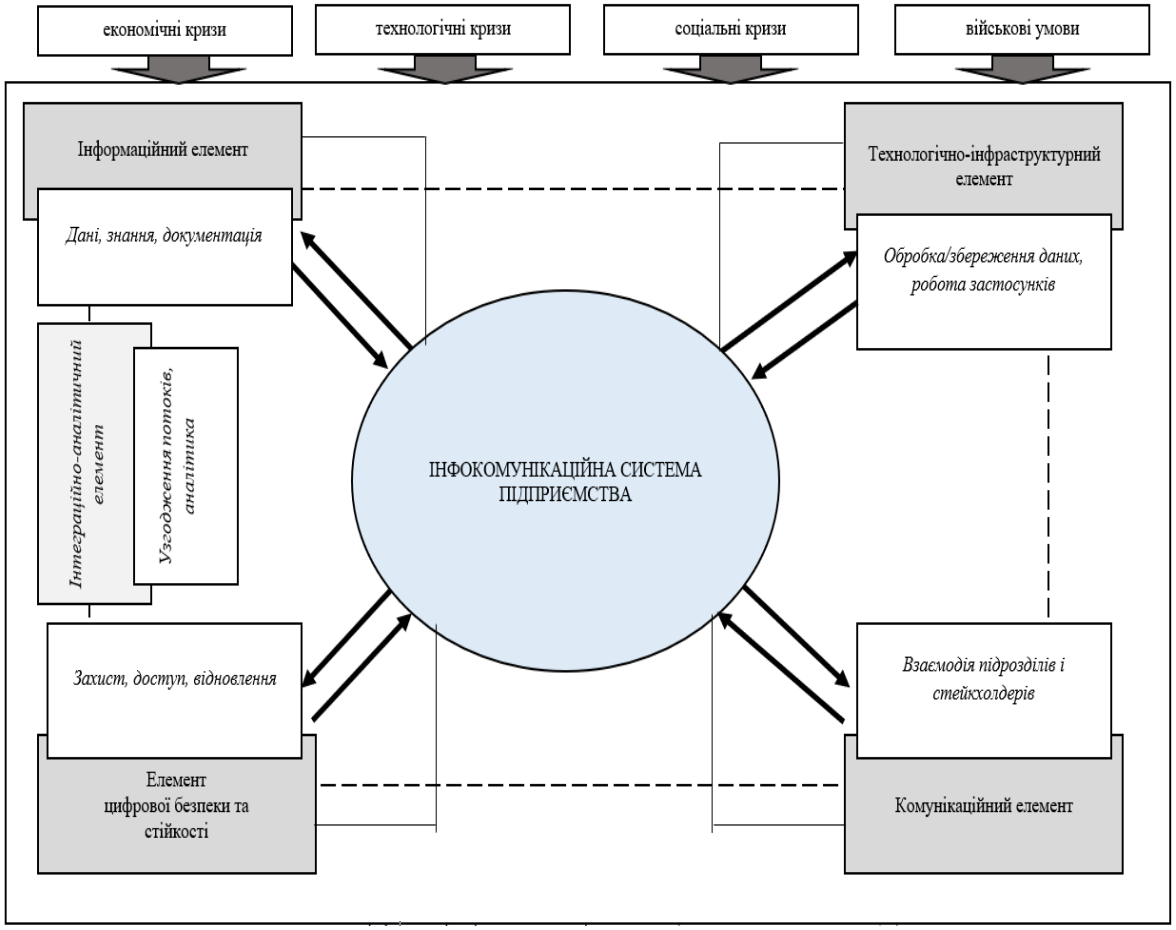

Рисунок 1. Структура інфокомунікаційної системи підприємства
Джерело: власна розробка автора

Вище відзначена структура інфокомунікаційної системи підприємства демонструє логіку її формування як узгодженої сукупності функціональних елементів, кожен з яких забезпечує окремий напрям цифрової взаємодії та підтримує стійкість підприємства в умовах зовнішніх викликів. Центральною ланкою виступає безпосередньо інфокомунікаційна система підприємства, яка координує і поєднує інформаційні, технологічні, комунікаційні, аналітичні та безпекові елементи та процеси в єдине управлінське цифрове середовище.

Інформаційний елемент охоплює ключові змістові компоненти цифрової діяльності – дані, знання та документацію – які становлять інформаційну базу для прийняття рішень. Технологічно-інфраструктурний елемент забезпечує технічне підґрунтя функціонування системи: підтримує роботу застосунків, оброб-

лення й збереження даних, мережеву взаємодію та інші технологічні операції. Комунікаційний елемент відповідає за організацію взаємодії між підрозділами та стейкхолдерами, сприяючи своєчасному та узгодженому обміну даними. Елемент цифрової безпеки та стійкості підтримує захищеність інформаційних процесів, контролює доступ, забезпечує відновлення та джерела цифрової надійності. Інтеграційно-аналітичний елемент виконує системоутворювальну роль, синхронізуючи інформаційні потоки, забезпечуючи їх узгодженість та створюючи аналітичну основу для обґрунтованих управлінських рішень.

Важливо підкреслити, що наведені елементи суттєво відрізняються від структури інфокомунікаційних ресурсів підприємства. Якщо ресурси відображають, що саме має підприємство (технології, дані, інфраструктуру, канали комунікації, засоби кіберзахисту), то елементи інфокомунікаційної системи характеризують, як ці ресурси взаємодіють у межах єдиного цифрового середовища. Іншими словами, ресурсний підхід визначає змістовне наповнення цифрової бази підприємства, тоді як системний підхід формує архітектуру їх функціонування, взаємопов'язаність та ролі у забезпеченні стійкості. Саме тому такі компоненти, як інтеграційно-аналітичний елемент або елемент стійкості, не є ресурсами у вузькому розумінні, але виникають як надбудова, коли ресурси об'єднуються в узгоджену схему.

Зовнішній контур рисунка охоплює чотири кризових викликів: економічні, технологічні, соціальні та військові кризи. Їх включення підкреслює, що інфокомунікаційна система функціонує не ізольовано, а постійно реагує на зовнішні ризики, які визначають вимоги до її гнучкості, надійності та адаптивності.

Відтак, у сукупності представлена модель демонструє, що лише взаємодія всіх елементів дозволяє підприємству використовувати свої цифрові ресурси максимально ефективно та підтримувати стійкість у мінливих умовах. Функціонування цифрової інфраструктури підприємства в сучасних умовах супроводжується зростанням кількості та складності ризиків, що впливають на доступність, цілісність та безперервність інформаційних процесів. На відміну від традиційних технічних загроз, сучасні ризики цифрового середовища мають комплексний характер, поєднуючи технологічні, організаційні, кібернетичні та зовнішні фактори, які здатні порушити роботу інфокомунікаційних систем і знизити загальну стійкість підприємства. В свою чергу вразливості виникають як на рівні технічних компонентів (мережеве обладнання, сервери, хмарні платформи), так і на рівні програмних застосунків, інтеграційних модулів, користувацького доступу та управління даними.

Особливої актуальності ці ризики набувають у контексті кризових ситуацій – економічних, технологічних, соціальних і військових – які посилюють нерівномірність навантажень на цифрові системи, підвищують ймовірність збоїв, перевантаження каналів зв'язку, кібератак чи втрати критично важливої інформації. За таких умов цифрова інфраструктура стає не лише технічною основою функціонування підприємства, а й потенційним джерелом системних загроз, здатних вплинути на ключові бізнес-процеси, фінансові результати й здатність підприємства та організації забезпечувати безперервність діяльності (табл. 1).

Таблиця 1. Ризики цифрової інфраструктури підприємств

Вид ризику	Характеристика	Приклад прояву
1. Технологічні	Виникають внаслідок збоїв у роботі апаратного та програмного забезпечення, порушень функціонування мережевих компонентів або інфраструктурних платформ	вихід з ладу серверів чи комутаторів, збої ERP/CRM, помилки у роботі хмарних рішень
2. Кібернетичні	Пов'язані з навмисним втручанням у цифрове середовище для порушення доступності, цілісності або конфіденційності даних	DDoS-атаки, шкідливе ПЗ, фішинг, викори-стання вразливостей у програмних компонентах
3.Організаційно-управлінські	Зумовлені недосконалістю внутрішніх регламентів, політик безпеки та управлінських процедур	неналежний розподіл прав доступу, відсут-ність політик резервного копіювання, недостатня цифрова компетентність персоналу
4.Інтеграційні	Виникають під час взаємодії між різними програмними модулям, сервісами або системами	конфлікти модулів ERP, помилки API, несумісність протоколів або даних
5. Зовнішні та кризові	Формуються внаслідок впливу зовнішнього середовища, що може порушувати роботу інфраструктури або збільшувати її навантаження	перебої електропостачання, фізичні руйнування об'єктів інфраструктури, воєнні загрози, регуляторні зміни

Джерело: складено автором за матеріалами [11-15]

Проведена деталізація дає змогу системно окреслити основні напрями ризиків, з якими стикається цифрова інфраструктура підприємства, та показує, що їх природа є багатовимірною й виходить за межі виключно технічних збоїв чи кібератак. Значна частина ризиків формується на стику технологічних, організаційних та інтеграційних процесів, що потребує комплексного підходу до їх виявлення та оцінювання. Важливо підкреслити, що кожна група ризиків по-різному впливає на інфраструктуру: технологічні загрози здебільшого порушують доступність цифрових сервісів, кібернетичні порушують конфіденційність і цілісність даних, організаційні створюють умовні «внутрішні точки» вразливості, тоді як зовнішні та кризові чинники здатні провокувати системні порушення в роботі інфокомунікаційної

системи. Відповідно до багатовекторного характеру цих загроз важливим є не лише класифікувати ризики, але й визначити їх конкретні джерела, можливі наслідки для підприємства та інструменти, що дають змогу мінімізувати вплив кожного з них (табл. 2).

Таблиця 2. Заходи мінімізації ризиків цифрової інфраструктури

Ризик	Джерело виникнення	Можливі наслідки для підприємства	Основні заходи мінімізації
1. Збій у роботі серверів або мережевого обладнання	Технічні помилки, зношеність обладнання, перевантаження інфраструктури	Зупинка бізнес-процесів, порушення доступності сервісів, втрата даних	Резервування серверів, кластеризація, моніторинг навантаження, заміна застарілого обладнання
2. Кібернетична атака (DDoS, шкідливе ПЗ, фішинг)	Зовнішні хакерські дії, відсутність належного захисту, людський фактор	Компрометація даних, порушення конфіденційності, фінансові втрати	Брандмауери, IDS/IPS, багаторівневий доступ, SOC-моніторинг, навчання персоналу
3. Інтеграційний збій між системами	Несумісність протоколів, помилки API, неправильні налаштування інтеграцій	Незбалансованість даних, збій операцій, зупинка критичних процесів	Стандартизація інтеграційних протоколів, тестування, резервні схеми оброблення
4. Помилки користувачів	Недостатня цифрова грамотність, порушення політик безпеки, людські помилки	Витік інформації, зміна або видалення даних, некоректні операції	Навчання персоналу, інструкції, контроль доступу, логування дій
5. Відсутність резервного копіювання або його нерегулярність	Ігнорування політик IT-безпеки, нестача ресурсів, слабке управління	Втрата критично важливої інформації, неможливість відновлення систем	Регламентоване резервне копіювання, зберігання копій у хмарі, періодичне тестування відновлення
6. Залежність від одного провайдера інтернет або хмарних послуг	Монополізація технологічної інфраструктури, відсутність альтернативних каналів	Повна недоступність сервісів у разі аварії провайдера	Мультиканальні схеми доступу, мультихмарна стратегія, SLA-контроль
7. Перебої електро-постачання або фізичні руйнування	Аварії, катастрофи , воєнні загрози	Зупинка IT-сервісів, пошкодження обладнання, простій підприємства	Генератори, переміщення частини інфраструктури у хмару
8. Регуляторні зміни та вимоги відповідності	Оновлення законодавства, нові стандарти захисту даних	Штрафи, обмеження діяльності, необхідність доробок систем	Юридичний моніторинг, аудит відповідності, адаптація політик та протоколів

Джерело: складено автором за матеріалами [13-17]

Представлені заходи узагальнюють ключові ризики цифрової інфраструктури та демонструють, що кожен із них має власну природу виникнення, характер впливу на роботу підприємства й специфічні механізми мінімізації. Відзначені взаємозв'язки між джерелами ризиків, можливими наслідками та відповідними заходами мінімізації дозволяють оцінити їх комплексний характер і сформувати цілісне бачення потенційних загроз для інфокомунікаційної системи. Зокрема технологічні та інтеграційні ризики здатні безпосередньо порушити безперервність роботи цифрових сервісів, тоді як кібернетичні загрози переважно впливають на конфіденційність і цілісність даних, а організаційні фактори створюють додаткові внутрішні передумови для матеріалізації інших видів ризиків.

Систематизація ризиків у такому форматі є важливою для подальшого визначення критичних вразливих точок цифрової інфраструктури, через які зазначені ризики можуть реалізуватися. Вразливості не лише відкривають шлях до матеріалізації загроз, але й відображають слабкі місця у структурі, процесах або політиках підприємства, що потребують підсилення. Проведемо класифікацію вразливостей цифрової інфраструктури, яка дозволяє точніше визначити, які саме фактори створюють ризикове середовище та яким чином вони впливають на загальний рівень цифрової стійкості підприємства (табл. 3).

Проведена класифікація вразливостей цифрової інфраструктури дозволяє виділити ключові слабкі місця, через які різні групи ризиків здатні реалізуватися та завдати суттєвої шкоди функціонуванню підприємства. Вразливості мають різну природу – від технічних недоліків обладнання або програмного забезпечення до організаційних прогалин, недостатньої цифрової грамотності персоналу чи помилок інтеграції між інформаційними системами. Саме поєднання цих чинників визначає загальний рівень стійкості інфокомунікаційної системи та ступінь її чутливості до зовнішніх і внутрішніх загроз.

Відтак, значущість виявлених вразливостей полягає у тому, що вони функціонують як «вхідні точки» для ризиків і визначають реальну ймовірність їх матеріалізації. Навіть за наявності сучасних технологій та розвиненої інфраструктури саме слабкі або недостатньо захищені елементи можуть спричинити масштабні

збої, порушення бізнес-процесів та втрату критично важливої інформації. У контексті виявлених ризиків і вразливостей особливої ваги набуває, яким чином інфокомунікаційні ресурси можуть бути задіяні для посилення стійкості підприємства, зменшення чутливості інфраструктури до загроз і забезпечення її безперервності.

Таблиця 3. Класифікація вразливостей цифрової інфраструктури підприємства

Група вразливостей	Характеристика	Типові прояви
1. Технічні	Порушення або слабкі місця в апаратному забезпеченні, мережевій інфраструктурі та фізичних компонентах системи.	Зношене або застаріле обладнання, відмова мережевих вузлів, відсутність резервування критичних компонентів.
2. Програмні	Недоліки, помилки чи закриті прогалини у програмному забезпеченні, які можуть бути використанні для порушення роботи системи.	Відсутність оновлень ПЗ, вразливості у кодуванні, помилки у конфігурації або патч-менеджменті.
3. Користувацькі	Слабкі місця, пов’язані з діями або помилками користувачів, що відкривають можливості для реалізації загроз.	Слабкі паролі або повторне використання доступів, фішингова поведінка, нехтування інструкціями безпеки.
4. Організаційні	Недостатня регламентація процесів, відсутність політик, процедур або контролю.	Відсутність чітких правил доступу, нерегулярне резервне копіювання, низька культура інформаційної безпеки.
5. Інтеграційні	Проблеми, що виникають під час взаємодії між різними системами, сервісами або модулями.	Помилки API-інтеграцій, несумісність протоколів, слабкі механізми контролю сторонніх постачальників.
6. Інфраструктурні	Слабкі місця у фізичній або мережевій інфраструктурі, що роблять системи чутливими до збоїв і зовнішніх чинників.	Залежність від одного провайдера, інтернету чи хмари, відсутність резервних каналів зв’язку, низька відмовостійкість мереж.
7. Процесуальні	Недоліки в організації процесів, що підтримують цифрову інфраструктуру, та в управлінні життєвим циклом ІТ-систем.	Слабкий контроль змін, відсутність планів реагування на інциденти, неузгоджені процеси техпідтримки.

Джерело: складено автором за матеріалами [16-20]

Ефективне використання інфокомунікаційних ресурсів є ключовим чинником підвищення стійкості підприємства до кризових впливів і забезпечення безперервності його діяльності. У сучасних умовах, коли швидкість поширення інформації, інтенсивність кібернетичних загроз та нестабільність зовнішнього середовища зростають, роль цифрових інструментів у запобіганні, виявленні та подоланні криз набуває особливої ваги. Інфокомунікаційні ресурси виступають не лише технічним забезпеченням функціонування бізнес-процесів, але й системоутворюючим елементом антикризового управління, що дає змогу оперативно реагувати на зміни, підтримувати критичні операцій та відновлюватися після деструктивних впливів.

Здатність підприємства протистояти кризам значною мірою залежить від того, наскільки ефективно організовані процеси збору, оброблення, аналізу та передачі інформації. У даному контексті інфокомунікаційні ресурси виконують комплекс функцій, спрямованих на забезпечення інформаційної прозорості, своєчасного виявлення загроз, координації дій між підрозділами, підтримки рішень та захисту критично важливих цифрових активів. Саме їх функціональне наповнення визначає можливості підприємства щодо запобігання негативним наслідкам кризових ситуацій і мінімізації ризиків, пов’язаних з порушенням роботи цифрової інфраструктури.

Така багатовекторність ролей інфокомунікаційних ресурсів зумовлює необхідність їх системного розгляду як цілісного функціонального механізму, що інтегрує інформаційні, технологічні, комунікаційні та безпекові компоненти. У кризових умовах кожен із цих компонентів виконує специфічні завдання: від раннього виявлення відхилень у роботі систем до забезпечення узгодженої взаємодії підрозділів і підтримки обґрунтованих управлінських рішень. У результаті інфокомунікаційні ресурси проявляють себе не лише як інструменти технічної підтримки, а як ключові елементи адаптивності, гнучкості та стійкості підприємства.

Важливим є і те, що функціональний потенціал цих ресурсів дозволяє підприємству не просто реагувати на кризові явища, а й формувати випереджувальну модель поведінки через аналітику, прогнозування, накопичення знань та створення резервних сценаріїв дій. Це підсилює здатність підприємства швидко відновлювати порушені процеси, мінімізувати втрати та забезпечувати керованість у період підвищеної турбулентності. З огляду на це доцільним є представити ключові функції інфокомунікаційних ресурсів, спрямованих на запобігання та подолання кризових явищ (рис. 2).

Рисунок 2. Функції інфокомунікаційних ресурсів у запобіганні та подоланні кризових явищ
Джерело: власна розробка автора

Представлена схема узагальнює ключові функції інфокомунікаційних ресурсів, що формують основу антикризового механізму підприємства. Кожна з них виконує окрему, але взаємопов'язану роль у забезпеченні стійкості підприємства до зовнішніх і внутрішніх загроз. Їх сукупна дія створює цілісне цифрове середовище, здатне підтримувати стабільність операцій, забезпечувати безперервність інформаційних потоків та сприяти швидкому відновленню бізнес-процесів після кризових впливів. Узагальнене та змістове наповнення цих функцій дозволяє визначити, яким чином інфокомунікаційні ресурси забезпечують проактивне управління ризиками та підвищують адаптивність підприємства в умовах турбулентності.

Функція моніторингу та раннього виявлення загроз забезпечує безперервний контроль стану цифрової інфраструктури та ідентифікацію відхилень, які можуть свідчити про наближення кризової ситуації. Використання інструментів моніторингу та аналізу дає змогу оперативно фіксувати порушення в роботі систем, підвищену активність у каналах зв'язку або спроби несанкціонованого доступу. Завдяки цьому підприємство здатне зменшити часовий лаг між появою загрози та реакцією на неї, що істотно скорочує масштаби потенційних збитків.

Функція координації та синхронізації дій підрозділів полягає у тому, що кризові явища потребують узгодженості рішень і швидкої взаємодії між структурними підрозділами. В свою чергу інфокомунікаційні ресурси створюють єдине інформаційне середовище, у межах якого здійснюється обмін повідомленнями, постановка завдань, фіксація дій і контролювання їх виконання. Це мінімізує дублювання операцій, зменшує хаотичність поведінки підприємства та дозволяє реалізовувати скоординовані заходи у відповідь на кризові впливи.

Функція відновлення та підтримки стійкості охоплює заходи, спрямовані на мінімізацію простоїв та швидке відновлення роботи цифрової інфраструктури після інцидентів. До її змісту належать резервування ресурсів, використання альтернативних каналів доступу, дублювання інформаційних систем та застосування процедур аварійного відновлення. Завдяки цьому забезпечується безперервність критично важливих функцій підприємства навіть у разі масштабних порушень.

Функція аналітичної підтримки управлінських рішень полягає у такому: аналітичні ресурси забезпечують керівництво підприємства достовірними даними, необхідними для оцінки ймовірності виникнення ризиків, визначення найбільш критичних напрямів впливу та вибору оптимальних дій у кризових умовах. Застосування систем бізнес-аналітики, інструментів машинного навчання та прогнозних моделей дозволяє формувати сценарії реагування, оцінювати їх ефективність та приймати обґрунтовані рішення під тиском часу та невизначеності.

У періоди криз кіберзагрози суттєво зростають, тому ключовим завданням інфокомунікаційних ресурсів є захист даних, інформаційних систем і каналів комунікації. Реалізація функції забезпечення кібербезпеки та захисту критичних активів включає контроль доступу, криптографічний захист, багаторівневу автентифікацію, виявлення загроз і моніторинг критичної активності. Це дозволяє запобігти втручанню, несанкціонованому доступу та пошкодженню цифрових активів підприємства.

Функція забезпечення інформаційної прозорості та безперервності обміну полягає у такому: інформаційна прозорість є критичною у періоди динамічності, коли своєчасність даних визначає ефективність оперативних рішень. Інфокомунікаційні ресурси підтримують стабільність інформаційних потоків, забезпечують доступ до актуальної інформації всім учасникам процесу, незалежно від їх локації чи режиму роботи. Це створює умови для оперативного реагування, зменшує ймовірність інформаційних розривів та забезпечує синхронність дій.

Кожна криза генерує унікальний досвід, який за належної фіксації може підвищити ефективність майбутнього реагування. Інфокомунікаційні ресурси створюють платформу для накопичення знань про

інциденти, документування процедур та формування бази найкращих практик. Саме тому функція інституціоналізації знань та накопичення досвіду кризового генерування сприяє розвитку організаційної пам'яті, стандартизації дій у повторюваних ситуаціях та підвищенню узгодженості антикризових процесів.

Висновки

Відтак, формування інфокомунікаційної структури підприємства в умовах кризових викликів набуває стратегічного значення, оскільки саме вона забезпечує можливість підтримувати стабільність, керованість та адаптивність ключових процесів у періоди підвищеної невизначеності. Сучасна інфраструктура має розглядатися як цілісний соціотехнічний комплекс, у межах якого поєднуються інформаційні, технологічні, комунікаційні, безпекові та інтеграційно-аналітичні елементи, що взаємодіють між собою для створення єдиного цифрового середовища. Кризові умови суттєво підсилюють вплив ризиків і вразливостей цифрової інфраструктури, що потребує систематизованого підходу до їх ідентифікації та оцінювання. Виявлені технологічні, кібернетичні, організаційні, інтеграційні та зовнішні ризики демонструють широкий спектр загроз, а класифікація вразливостей підкреслює важливість урахування не лише технічних, але й процесуальних, користувацьких та інфраструктурних аспектів.

Це формує підґрунтя для розроблення дієвих механізмів захисту та підвищення стійкості цифрового середовища підприємства. Тим самим інфокомунікаційна інфраструктура в умовах викликів постає як стратегічний елемент забезпечення цифрової стійкості підприємства. Її ефективне формування та управління дозволяє мінімізувати вразливості, підвищити готовність до зовнішніх впливів та забезпечити безперервність критичних бізнес-процесів у довгостроковій перспективі.

Abstract

The information and communication infrastructure serves as an integrating basis for the processing, transmission and use of the enterprise's information resources, ensuring the interconnection between management, production and communication subsystems. In times of crisis, its role increases significantly, as it is digital and information and communication solutions that enable a rapid response to changes in the external environment, minimise losses, maintain the manageability of organisational structures and preserve competitiveness. Despite the existence of a significant number of scientific studies devoted to digitalisation and information technologies in the activities of enterprises, the issue of the holistic formation of an information and communication infrastructure, taking into account crisis conditions, remains insufficiently systematised.

The structure of an enterprise's information and communication system demonstrates the logic of its formation as a coordinated set of functional elements, each of which provides a separate direction of digital interaction and supports the stability of the enterprise in the face of external challenges. The central link is the enterprise's information and communication system, which coordinates and combines information, technological, communication, analytical and security elements and processes into a single digital management environment. The functioning of an enterprise's digital infrastructure in today's environment is accompanied by an increase in the number and complexity of risks affecting the availability, integrity and continuity of information processes. Unlike traditional technical threats, modern risks in the digital environment are complex in nature, combining technological, organisational, cybernetic and external factors that can disrupt the operation of information and communication systems and reduce the overall resilience of the enterprise. A significant part of the risks is formed at the intersection of technological, organisational and integration processes, which requires a comprehensive approach to their identification and assessment. It is important to emphasise that each group of risks affects the infrastructure in different ways: technological threats mainly disrupt the availability of digital services, cyber threats compromise data confidentiality and integrity, organisational threats create conditional 'internal points' of vulnerability, while external and crisis factors can cause systemic disruptions in the operation of the information and communication system.

The classification of digital infrastructure vulnerabilities allows us to identify key weaknesses through which various risk groups can materialise and cause significant damage to the functioning of an enterprise. Vulnerabilities vary in nature, ranging from technical deficiencies in equipment or software to organisational gaps, insufficient digital literacy of personnel, or integration errors between information systems. It is the combination of these factors that determines the overall level of resilience of the information and communication system and its sensitivity to external and internal threats. key functions of information and communication resources that form the basis of the enterprise's crisis response mechanism. Each of them plays a separate but interrelated role in ensuring the enterprise's resilience to external and internal threats. Their combined action creates a holistic digital environment capable of maintaining operational stability, ensuring the continuity of information flows, and facilitating the rapid recovery of business processes after crisis impacts.

Список літератури:

1. Mohammed A. N. N. A. M., Hu W. Using Management Information Systems (MIS) to Boost Corporate Performance. The international journal of management science and business administration. 2015. Vol. 1, No. 11. P. 55-61. DOI: 10.18775/ijmsba.1849-5664-5419.2014.111.1006.
2. Lusianah, Meiryani. The Role of Management Information Systems in Achieving Excellent Operational Performance. International Journal of Scientific & Technology Research. 2019. Vol. 8, No. 4. P. 304-306.
3. Huber G. Organizational Information Systems: Determinants of Their Performance and Behavior. Management Science. 1982. №28(2). P. 138-155. URL: http://www.jstor.org/stable/2631299.
4. Tarigan Z. J. H., Siagian H., Jie F. Impact of Enhanced Enterprise Resource Planning (ERP) on Firm Performance through Green Supply Chain Management. Sustainability. 2021. №13(8). DOI: 10.3390/su13084358.
5. Voulgaris F., Lemonakis C., Papoutsakis M. The Impact of ERP Systems on Firm Performance: The Case of Greek Enterprises. Global Business and Economics Review. 2015. Vol. 17, No. 1. P. 112-129. DOI: 10.1504/GBER.2015.066536.
6. Chen X., Dai Q., Na C. The Value of Enterprise Information Systems Under Different Corporate Governance Aspects. Information Technology and Management. 2019. №20. P. 223-247. DOI: 10.1007/s10799-019-00310-3.
7. Berente N., Lyytinen K., Yoo Y., King J. L. Routines as Shock Absorbers During Organizational Transformation: Integration, Control, and NASA's Enterprise Information System," Organization Science, INFORMS. 2016. Vol. 27(3). P. 551-572. DOI: 10.1287/orsc.2016.1046.
8. Mentzas G. Towards Intelligent Organisational Information Systems. International Transactions in Operational Research. 1994. Vol. 1, No. 2. P. 169-187. DOI: 10.1016/0969-6016(94)90018-3.
9. Saarinen T. Evolution of information systems in organizations. Behaviour & Information Technology. 1989. №8(5). P. 387-398. DOI: 10.1080/01449298908914568.
10. Kanellou A., Spathis C. Accounting Benefits and Satisfaction in an ERP Environment. International Journal of Accounting Information Systems. 2013. Vol. 14, No. 3. P. 209-234. DOI: 10.1016/j.accinf.2012.12.002.
11. McCallister E., Grance T., Scarfone K. Guide to protecting the confidentiality of personally identifiable information. Recommendations of the National Institute of Standards and Technology. 2009. 58 p.
12. Shameli-Sendi A., Aghababaei-Barzegar R., Cheriet M. Taxonomy of information security risk assessment (ISRA). Computers & Security. Vol. 57. P. 14-30. DOI: 10.1016/j.cose.2015.11.001.
13. Frolova L., Gorodetska T., Ivanchuk K., Zaychenko K., Nosova T. Freelance as the main trend in doing business in the food industry. Journal of Hygienic Engineering and Design, 2018. Vol. 25, pp. 81-86.
14. Fenz, S., Ekelhart, A. Formalizing information security knowledge. In Proceedings of the 2009 ACM symposium on Information, computer and communications security. 2009. P. 183-194.
15. Башинська І.О. Удосконалення системи управління ризиками на підприємстві. Причорноморські економічні студії. 2017. № 17. С. 91-94.
16. Shedden, P., Ahmad, A., Smith, W. Information security risk assessment: Towards a business practice perspective. Proceedings of the 8th Australian Information Security Management Conference. 2010. P. 119-130.
17. Ahmad, A., Maynard, S. B., Shanks, G. A case analysis of information systems security incident responses. International Journal of Information Management. 2015. Vol. 35, No. 6. P. 717-723.
18. Böhme, R., Kataria, G. Models and Measures for Correlation in Cyber-Insurance. Workshop on the Economics of Information Security. 2006. URL: https://www.semanticscholar.org/paper/Models-and-Measures-for-Correlation-in-Böhme-Kataria/24af7e7832277628c9fa108e31c31d75d3c494bc.
19. Tankard, C. Advanced Persistent Threats and How to Monitor and Deter Them. Network Security. 2011. Vol. 2011 №8. P. 16-19.
20. Башинська І.О., Валянська А.О., Гомонюк Г.І. Управління ризиками як напрям забезпечення конкурентоспроможності підприємств. Молодий вчений. 2019. № 1(2). С. 413-416.

References:

1. Mohammed, A. N. N. A. M., & Hu, W. (2015). Using management information systems (MIS) to boost corporate performance. The International Journal of Management Science and Business Administration, 1(11), 55-61. DOI: 10.18775/ijmsba.1849-5664-5419.2014.111.1006 [in English].
2. Lusianah, & Meiryani. (2019). The role of management information systems in achieving excellent operational performance. International Journal of Scientific & Technology Research, 8(4), 304-306 [in English].

3. Huber, G. (1982). Organizational information systems: Determinants of their performance and behavior. Management Science, 28(2), 138-155. Retrieved from: http://www.jstor.org/stable/2631299 [in English].
4. Tarigan, Z. J. H., Siagian, H., & Jie, F. (2021). Impact of enhanced enterprise resource planning (ERP) on firm performance through green supply chain management. Sustainability, 13(8). DOI: 10.3390/su13084358 [in English].
5. Voulgaris, F., Lemonakis, C., & Papoutsakis, M. (2015). The impact of ERP systems on firm performance: The case of Greek enterprises. Global Business and Economics Review, 17(1), 112-129. DOI: 10.1504/GBER.2015.066536 [in English].
6. Chen, X., Dai, Q., & Na, C. (2019). The value of enterprise information systems under different corporate governance aspects. Information Technology and Management, 20, 223-247. DOI: 10.1007/s10799-019-00310-3 [in English].
7. Berente, N., Lyytinen, K., Yoo, Y., & King, J. L. (2016). Routines as shock absorbers during organizational transformation: Integration, control, and NASA's enterprise information system. Organization Science, 27(3), 551-572. DOI: 10.1287/orsc.2016.1046 [in English].
8. Mentzas, G. (1994). Towards intelligent organisational information systems. International Transactions in Operational Research, 1(2), 169-187. DOI: 10.1016/0969-6016(94)90018-3 [in English].
9. Saarinen, T. (1989). Evolution of information systems in organizations. Behaviour & Information Technology, 8(5), 387-398. DOI: 10.1080/01449298908914568 [in English].
10. Kanellou, A., & Spathis, C. (2013). Accounting benefits and satisfaction in an ERP environment. International Journal of Accounting Information Systems, 14(3), 209-234. DOI: 10.1016/j.accinf. 2012.12.002 [in English].
11. McCallister, E., Grance, T., & Scarfone, K. (2009). Guide to protecting the confidentiality of personally identifiable information. National Institute of Standards and Technology [in English].
12. Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & Security, 57, 14-30. DOI: 10.1016/j.cose.2015.11.001 [in English].
13. Frolova, L., Gorodetska, T., Ivanchuk, K., Zaychenko, K., & Nosova, T. (2018). Freelance as the main trend in doing business in the food industry. Journal of Hygienic Engineering and Design, 25, 81-86 [in English].
14. Fenz, S., & Ekelhart, A. (2009). Formalizing information security knowledge. In Proceedings of the 2009 ACM Symposium on Information, Computer and Communications Security (pp. 183-194). ACM [in English].
15. Bashynska, I.O. (2017). Improvement of enterprise risk management system. Prychornomorski Ekonomichni Studii, 17, 91-94 [in Ukrainian].
16. Shedden, P., Ahmad, A., & Smith, W. (2010). Information security risk assessment: Towards a business practice perspective. In Proceedings of the 8th Australian Information Security Management Conference (pp. 119-130) [in English].
17. Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems security incident responses. International Journal of Information Management, 35(6), 717-723 [in English].
18. Böhme, R., & Kataria, G. (2006). Models and measures for correlation in cyber-insurance. Workshop on the Economics of Information Security. Retrieved from: https://www.semanticscholar.org/paper/Models-and-Measures-for-Correlation-in-Böhme-Kataria/24af7e7832277628c9fa108e31c31d75d3c494bc [in English].
19. Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. Network Security, 2011(8), 16-19 [in English].
20. Bashynska, I.O., Valianska, A.O., & Homoniuk, H.I. (2019). Risk management as a direction of ensuring enterprise competitiveness. Molodyi Vchenyi, 1(2), 413-416 [in Ukrainian].

Посилання на статтю:
Алі Рашид Халіфа Бумекайр Альмансурі. Формування інфокомунікаційної інфраструктури підприємства в умовах криз / Алі Рашид Халіфа Бумекайр Альмансурі // Економічний журнал Одеського політехнічного університету. – 2025. – № 1 (31). – С. 136-145. – Режим доступу до журн.: https://economics.net.ua/ejopu/2025/No1/136.pdf.
DOI: 10.15276/EJ.01.2025.14. DOI: 10.5281/zenodo.18025510.

Reference a Journal Article:
Ali Rashed Khalifa Bumeqairaa Almansoori. Formation of an Enterprise's Information and Communication Infrastructure in Crisis Conditions / Ali Rashed Khalifa Bumeqairaa Almansoori // Economic journal Odessa polytechnic university. – 2025. – № 1 (31). – P. 136-145. – Retrieved from https://economics.net.ua/ejopu/2025/No1/136.pdf.
DOI: 10.15276/EJ.01.2025.14. DOI: 10.5281/zenodo.18025510.