УДК 004.056.5 **doi:** https://doi.org/10.20998/3083-6298.2025.01.03

Ольга Король[1], Ірина Аксьонова[1], Єлизавета Севрюкова[2]

[1] Національний технічний університет «Харківський політехнічний інститут»”, Харків, Україна
[2] Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна

# РОЗРОБКА МЕТОДУ ОЦІНКИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕС-ПРОЦЕСІВ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

**Анотація. Актуальність** дослідження зумовлена зростаючою залежністю об'єктів критичної інфраструктури від інформаційних технологій та інтенсифікацією кіберзагроз, що спричиняють суттєві ризики для безперервності бізнес-процесів. Особливо вразливими є організації банківського сектора, для яких навіть короткочасне припинення роботи може призвести до значних фінансових та репутаційних втрат. **Предметом вивчення** є підходи, стратегії та показники оцінювання рівня забезпечення безперервності бізнес-процесів в умовах реалізації кіберзагроз, а також вплив факторів безпеки на ефективність функціонування об'єктів критичної інфраструктури. **Метою статті** є вивчення підходів до забезпечення стійкої роботи бізнес-процесів організацій банківського сектора в умовах зростаючих кіберзагроз шляхом аналізу механізмів удосконалення систем попередження дій терористичного характеру, спрямованих на об'єкти критичної інфраструктури. У **результаті** проведеного дослідження: проаналізовано характер та засоби реалізації кіберзагроз терористичного спрямування до об'єктів критичної інфраструктури; виділено ключові стратегії забезпечення безперервності бізнесу та визначено релевантні показники для їх оцінювання; запропоновано підхід до оцінки впливу стратегічних рішень на рівень безперервності бізнес-процесів; розроблено загальну структуру методу, що дозволяє моделювати та оцінювати стійкість функціонування організацій банківського сектору в умовах дестабілізаційних факторів. **Висновок.** Дослідження дозволяє підвищити обґрунтованість управлінських рішень щодо вибору стратегій забезпечення безперервності. Запропонований підхід може бути використаний як основа для створення методичних рекомендацій з управління кіберризиками в критично важливих секторах економіки.

**Ключові слова:** кібертероризм, кібератака, критична інфраструктура, безперервність бізнес-процесів, безпека банківського сектору

## 1. Вступ

**Актуальність проблеми та аналіз літературних джерел.** Розвиток суспільства у XXI столітті характеризується, в першу чергу, стрімким переходом від інформаційного суспільства до суспільства високих технологій, що забезпечують перенасиченість новітніми інформаційними та комунікаційними технологіями, подальший розвиток глобалізаційних процесів у сучасній економіці, динаміку інформатизації таких областей діяльності суспільства, як сфера зв’язку, енергетика, транспорт, системи видобутку та зберігання нафти і газу, фінансова та банківська системи, оборонна та національна безпека, забезпечення стабільної роботи державних структур, перехід на методи електронного управління та документообігу [1,2]. В другу чергу, цифровізаційні процеси, що відбуваються в усьому світі, висувають на перший план найважливішу задачу забезпечення безпеки інформації. Це пояснюється особливою значущістю для розвитку держави його інформаційних ресурсів, зростанням вартості інформації в умовах діджиталізації, її високою вразливістю та значними збитками у результаті несанкціонованого використання [1-4]. В третю чергу, бурхливий розвиток цифровізації суспільства, Інтернет-технологій формує глобальний інформаційний простір, що дозволяє створювати нові загрози та нові форми міжнародних конфліктів, включаючи інформаційні війни, мережеві протиборства, хакерські атаки та інше. Розвиток комп'ютерних технологій та інформаційно-телекомунікаційних мереж дають більші можливості суспільсту, в той же час створюють і новий вид злочинів – кіберзлочини [5,6]. Так, у 2015 році терористична організація «Ісламська держава Ірака і Леванта» (ІДІЛ) створила підрозділ, що займається проведенням комп'ютерних атак. У мережі Інтернет даний підрозділ відомий під назвою Cyber Caliphate, основними цілями якого є злам і розкриття конфіденційної інформації, атаки на інтернет-ресурси, в число яких входять сайти банків, наукових центрів, державних підприємств та ін. [7,8]. Про ступінь небезпеки електронних порушень для суспільства можна судити за тими витратами на засоби захисту, які вважаються допустимими та доцільними. За оцінками фахівців з безпеки електронного документообігу США, загальні витрати на захист банківських або інших фінансових установ можуть скласти всього близько 510 тис. доларів. Однак вважається, що надійна система захисту великої фінансової установи, яка обслуговує до 80000 клієнтів, коштує не менше 15 млн доларів, причому в цю суму входять тільки витрати на апаратні та програмні кошти (без урахування оплати праці найманого штату фахівців з безпеки) [9].

**Мета дослідження** полягає в розгляді завдань забезпечення безперервності бізнес-процесів в організаціях банківського сектора (ОБС) в умовах збільшення кібергроз, на основі аналізу способів удосконалення попереджень терористичної спрямованості на об’єкти критичної інфраструктури. Для досягнення мети вирішуються такі завдання:

1) аналіз сучасних способів вчинення злочинів терористичної спрямованості, зокрема кібертерористичних атак, спрямованих на об'єкти критичної інформаційної інфраструктури, та визначення характерних сценаріїв загроз для

організацій банківського сектору;

2) ідентифікація особливостей функціонування критичної інформаційної інфраструктури в контексті безперервності бізнес-процесів, визначення її вразливих місць до кіберзагроз та впливів потенційних атак на стабільність роботи ОБС.

3) розробка та систематизація стратегій забезпечення безперервності бізнесу в організаціях банківського сектора, а також визначення ключових кількісних та якісних показників оцінки ефективності заходів із запобігання порушенням у роботі критичної інфраструктури.

## 2. Основна частина

**2.1. Аналіз способів скоєння злочинів терористичного спрямування на об'єкти критичної інфраструктури**. Інформаційні загрози можуть проявляти себе у різних формах. Кібертероризм характеризується прагненням до суттєвої дестабілізації суспільного ладу. Дане явище нерозривно пов'язане з розвитком інформаційної інфраструктури: при постійно зростаючій залежності суспільства від безперебійного функціонування обчислювальних систем, дії, спрямовані на їх руйнування, завдають все більшої шкоди та викликають серйозний суспільний резонанс [10]. При цьому під кібертероризмом розуміють цілеспрямоване залякування населення та органів влади реальними або можливими та проголошеними (заявленими) кібернетичними впливами на соціум, соціотехнічні та технічні системи, здійснення яких призводить до виникнення (створення передумов для виникнення) небезпеки для громадян, суспільства, держави [1,3]. Особливе занепокоєння в останнє десятиліття викликає використання міжнародним тероризмом для реалізації терористичних акцій існуючих інформаційних ресурсів, насамперед, мережі Інтернет. Глобальна мережа приваблює терористичні групи такими своїми особливостями [11-13]:

оперативністю, економічністю та доступністю;

слабкою цензурою або повною відсутністю її та будь-якого контролю з боку держави;

наявністю величезної потенційної аудиторії користувачів, розкиданої по всьому світу;

швидким та відносно дешевим поширенням спеціально підібраної інформації, комплексністю її подання та сприйняття (розсилання електронних листів e-mail, організація груп новин, створення сайтів для обміну думками, розміщення інформації на окремих сторінках або в електронних версіях періодичних видань та мережевого мовлення та ін.);

можливістю користувачам працювати відносно конфіденційно та анонімно завдяки потужностям серверів комунікаційних мереж;

можливістю використання спеціальних роботів (bots) для зниження часу та витрат на терористичну діяльність;

високою ефективністю наслідків, які можуть мати як локальний, так і глобальний характер;

складністю відстеження кіберзлочинів та збору доказів злочину;

невизначеністю місця, часу та процесу підготовки до здійснення кібертеракту;

можливістю організації актів кібертерору одночасно на різні об'єкти або суб'єкти з різних напрямків без необхідності порушення будь-яких кордонів;

можливістю несанкціонованого підключення до комп'ютерних мереж управління стратегічними об'єктами, зокрема військовими;

високим ступем анонімності при здійсненні кібертерактів;

просторово-тимчасовою віддаленістю від об'єкта або суб'єкта кібератаки. Всі кібернетичні впливи здійснюються в кіберпросторі та безпосередньо через кіберпростір.

Основні засоби кібертероризму представлені на рис. 1.

Аналіз рис. 1 показує що, тероризм все більше стає інформаційною технологією особливого типу, оскільки, терористи все ширше використовують можливості сучасних інформаційно-телекомунікаційних систем для зв'язку та збору інформації, більшість терористичних актів розраховані не тільки на заподіяння матеріальних збитків і загрози життю і здоров'ю людей, але й на інформаційно-психологічний шок, вплив якого на велику кількість людей створює сприятливе середовище для досягнення терористами своїх цілей.

Таким чином, в умовах нарощування в світі процесів глобалізації та формування інформаційного суспільства тероризм став виступати як самостійний фактор, здатний загрожувати державній цілісності країн і дестабілізувати міжнародну обстановку. Терористичні групи використовують можливості новітніх інформаційних технологій для розповсюдження пропаганди та обміну інформацією, залучення нових зловмисників, фінансових вкладень для підтримки, планування терактів, і, навіть, для здійснення контролю над їх проведенням [14].

Основні напрями використання новітніх інформаційних технологій та мережі Інтернет у терористичних цілях наведено на рис. 2.

Проведений аналіз рис. 2 показав, що соціальні мережі активно використовуються для пропаганди демонстрації життя бойовиків, військового способу життя та героїзму бойовиків, заклику боротися за свої ідеали зі зброєю в руках, трансляції сцен вдалих бойових дій та актів залякування. Фото та відеозвіти супроводжуються піснями з відповідним змістом, які займають важливе місце у формованій культурної матриці глобальної терористичної спільноти. У терористичних груп є власні мобільні додатки та інтернет-магазини, де можна придбати товари з їх логотипом. Вся ця небезпечна для свідомості продукція поширюються багатьма мовами світу.

Активне використання терористами кіберпростору в Європі показало наступну картину [14]: 84% молодих людей прийшли до лав терористичних організацій через мережу Інтернет; 47% – звернули увагу на матеріали (відео, текст), розміщені онлайн; 41% – присягнули на вірність терористичним організаціям онлайн; 19% –

користувалися онлайн-інструкціями під час підготовки теракту (виготовлення саморобних вибухових пристроїв та бомб). Основне завдання подібних продуктів – залучити та зацікавити нових учасників, втягнути їх у спілкування у форматі питання-відповідь з метою психологічної обробки для подальшої ізоляції людини від близького оточення та соціуму в цілому та залучення до лав терористів.

Таким чином, на відміну від традиційного тероризму, який не загрожував суспільству як такому і не торкався основ його життєдіяльності, сучасний високотехнологічний тероризм здатний продукувати системну кризу в будь-якій державі з високорозвиненою інформаційною інфраструктурою. Розвиток соціальних мереж супроводжується все більш широким використанням їх можливостей для здійснення інформаційного протиборства, зростанням координації, масштабів та складності дій його учасників, якими найчастіше виступають як держави, так і окремі організовані групи, у т. ч. терористичні. Об'єктом кібератак дедалі частіше стають інформаційні ресурси, виведення з ладу чи “утруднення” функціонування яких може завдати значний економічний збиток чи викликати великий суспільний резонанс [13,14].


**Рис. 1.** Основні засоби кібертероризма

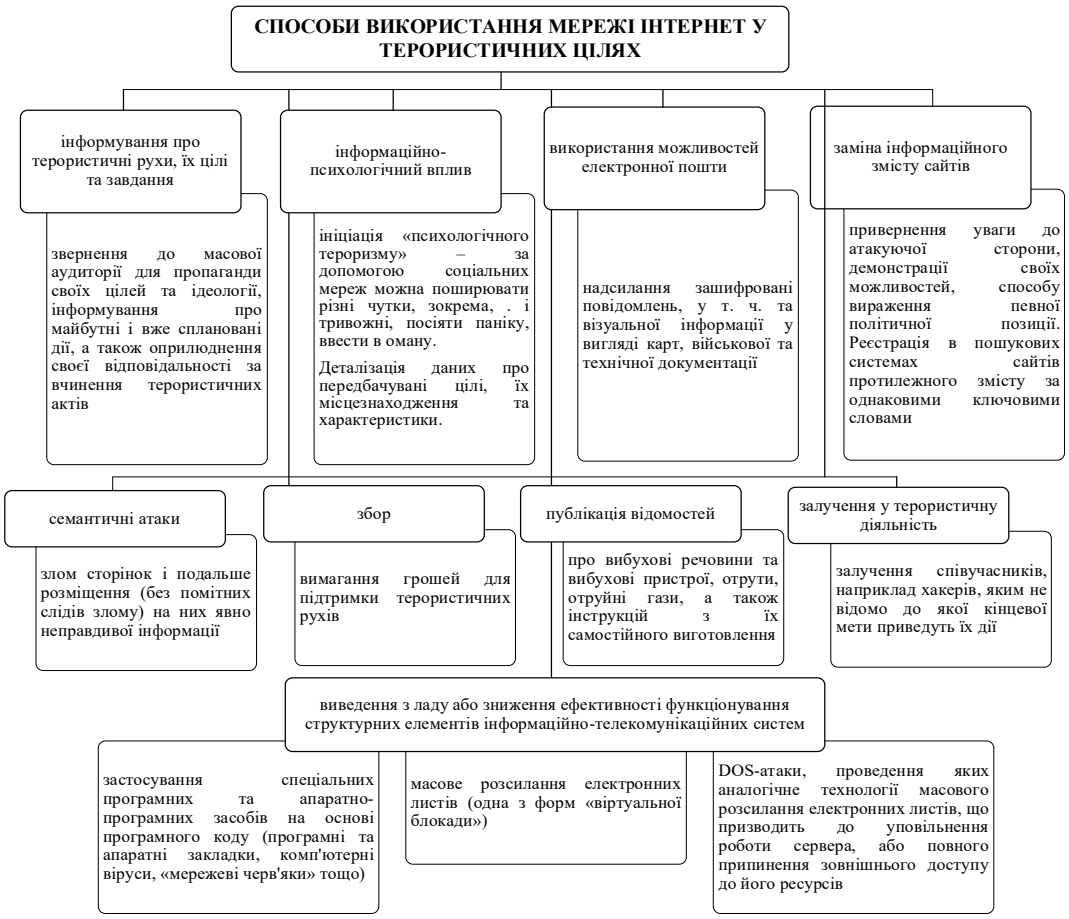


**Рис. 2.** Основні способи використання мережі Інтернет

**2.2. Критичні інформаційні інфраструктури.** Використання терористами новітніх розробок у сфері інформаційно-комунікаційних технологій дозволяють радикально змінювати методи терористичної діяльності, формувати гнучкі та ефективні мережеві організаційні структури, що об'єднують окремі групи у транснаціональні терористичні угруповання, які дуже важко виявити до здійснення терористичного акту. Інформаційні атаки зазвичай поділяються на дві категорії: виведення з ладу інформаційних ресурсів та руйнівні атаки. Руйнівні атаки [13,15] – це інформаційні (хакерські) операції проти об'єктів, які можуть знищити інформаційний ресурс, лінії комунікації, або викликати фізичне знищення структур, які включають інформаційні системи. Якщо системи діють у критичних інфраструктурах, то за найгіршого розвитку подій мережеві інформаційні атаки можуть мати масштабні наслідки з людськими жертвами, як і традиційні терористичні акти.

Критично важлива інфраструктура має ключове значення для громадського порядку, економічної стабільності та національної безпеки держав, її захист торкається питань національної безпеки, і тому входить до компетенції держави. Тим не менш, велика частина інфраструктур перебуває у власності приватного бізнесу, тому держава та бізнес змушені спільно нести відповідальність за безпеку та стабільне функціонування цих систем [4].

На сьогоднішній день держави самостійно визначають, що відносити до критично важливих інфраструктур, залежно від економічного стану держави, політичного керівництва, географічних та історичних особливостей. В Україні на законодавчому та нормативному рівні не надано визначення критично важливих об'єктів та ключових систем інформаційної інфраструктури. Враховуючи аналіз публікацій фахівців із США, ряду країн Європи, автори [16] пропонують узагальнені визначення критично важливих об'єктів (КВО) та критично важливої інформаційної інфраструктури України (КВІІ).

Критично важливий об'єкт – це об'єкт, порушення (або припинення) функціонування якого призводить до втрати управління, руйнування інфраструктури, незворотної негативної зміни (або руйнування) економіки країни або адміністративно-територіальної одиниці або суттєвого погіршення безпеки життєдіяльності населення, яке проживає на цих територіях, на тривалий термін [16].

Ключова система інформаційної інфраструктури – це інформаційно-керуюча або інформаційно-телекомунікаційна система, що відповідає одній із вимог [16]:

здійснює управління КВО (процесом);

здійснює інформаційне забезпечення управління КВО (процесом);

здійснює інформування громадян щодо надзвичайних ситуацій.

Таким чином, головною характеристикою критичної інфраструктури є її ключове значення для безпеки суспільства та держави. Критично важливі інфраструктури можуть мати подвійне призначення і ставитися як до КВО військового призначення, так і до КВО цивільного призначення. У табл. 1 наведено співвідношення критичних інфраструктур держав України та США.

*Таблиця 1* – **Критично важливі інфраструктури держав України та США за призначенням**

| КВО України | КВО США |
|---|---|
| Цивільні об'єкти | |
| охорона здоров'я | здоров'я суспільства |
| Об'єкти подвійного призначення | |
| сільське господарство | харчування та сільське господарство |
| водопостачання | вода |
| державне управління | державне управління |
| інформаційні та телекомунікаційні мережі | інформаційні та телекомунікаційні мережі |
| енергетичні системи | енергетичні системи |
| банківська та фінансові системи | банківська та фінансові системи |
| хімічна промисловість | хімічна промисловість та вибухонебезпечні матеріали |
| теплопостачання | – |
| транспортна система | наземний та водний транспорт |
| індустріальна промисловість | критично важливе виробництво |
| цивільна оборона | служби екстреного реагування |
| Військові об'єкти | |
| військово-промисловий комплекс | військово-промисловий комплекс |

Отже, аналіз табл. 1 показує, що ОБС відносяться до КВО, а автоматизована банківська система забезпечує автоматизацію і безперервність бізнес-процесів, обробку, зберігання та передачу великих обсягів банківської інформації, необхідних для діяльності ОБС, отже, від надійності та безпеки функціонування інформаційної інфраструктури автоматизованої банківської системи безпосередньо залежить безперервність бізнес-процесів, доступність і цілісність банківської інформації, а, отже, і діяльність ОБС в цілому.

Аналіз та узагальнення існуючого досвіду антитерористичної діяльності дозволив сформулювати завдання щодо захисту критичної інфраструктури від кібертероризму та основні заходи, спрямовані на їх вирішення, які представлені в табл. 2 [1,4,13,16,17]. Комплексне вирішення перелічених завдань дозволить вживати в централізованому порядку необхідні контрзаходи для протидії кібертероризму, суттєво знизити ймовірність реалізації його загроз щодо критичної інфраструктури та забезпечити захист своїх національних інтересів.

*Таблиця 2* – **Основні заходи, спрямовані на запобігання кіберзлочинності**

| На національному рівні | На міжнародному рівні |
|---|---|
| 1 | 2 |
| організація моніторингу та прогнозування потреб економічних та інших структур у різних видах інформаційного обміну через мережі Інтернет | організація міждержавного співробітництва у роботі міжнародних організацій, громадських комітетів та комісій у проєктах розвитку світових інформаційних мереж |
| координація заходів державних та недержавних відомств щодо запобігання загроз інформаційній безпеці у відкритих мережах. Розробка єдиної політики, що передбачає захист мережевого обладнання на території країни від проникнення до нього прихованих елементів інформаційної зброї | активна участь у розробці міжнародного законодавства та нормативно-правового забезпечення функціонування глобальних мереж відкритої інфраструктури |
| розробка державної програми вдосконалення інформаційних технологій, що забезпечують підключення національних та корпоративних мереж до відкритих мереж | створення єдиного антитерористичного простору країн-союзників |
| вдосконалення технологій своєчасного виявлення та нейтралізації несанкціонованого доступу до інформації, створення та використання випереджальних технологій | розробка науково-методичного забезпечення з припинення транснаціональних терористичних атак з використанням глобальних мереж, вироблення єдиного понятійного апарату, шкали оцінки кіберзагроз та їх наслідків |
| розробка національного законодавства щодо правил поводження з інформаційними ресурсами, регламенту прав, обов'язків та відповідальності користувачів мереж відкритої інфраструктури | вироблення механізмів взаємного інформування про широкомасштабні комп'ютерні атаки та великі інциденти в кіберпросторі, а також способів спільного реагування на загрози кібертероризму |
| встановлення переліку інформації, що не підлягає передачі по відкритих мережах, та забезпечення контролю за дотриманням встановленого статусу інформації | уніфікація національних законодавств у сфері захисту критичної інфраструктури від кібертероризму |

**2.3. Стратегії та показники забезпечення безперервності бізнес-бізнесу в автоматизованій банківській системі ОБС.** У будь-якій соціальній сфері (до якої належить і сфера безпеки банківської інформації в автоматизованій банківській системі

ОБС) інциденти безпеки, переривання роботи та аварії є неминучими. Однак їх вплив на діяльність компанії має бути мінімізовано: дані мають бути збережені, технічні засоби перебувати у робочому стані, репутація врятована, люди – знаходитись поза небезпекою [18,19]. Вирішення зазначених завдань можливо здійснити в рамках управління безперервністю бізнесу – цілісного процесу управління, в межах якого ідентифікуються потенційні загрози діяльності організації, оцінюються можливі впливи на бізнес-операції у разі реалізації цих загроз, а також створюється система приписів для забезпечення здатності організації відновлювати свою діяльність та ефективно реагувати на інциденти, що забезпечує захист репутації, бренду та створює цінність операцій. [20].

Можна виділити два основних інструменти безперервності бізнес-процесів [18-20]:

план безперервності бізнесу (BCP) – набір превентивних заходів, детальних інструкцій для дій у гострих (критичних) ситуаціях, в ОБС додатково розглядаються заходи по відновленню банківської інформації;

планування аварійного відновлення (DRP) – підготовка організації до якнайшвидшого повного відновлення її діяльності у разі аварії, атаки, кризової ситуації тощо.

Незважаючи на відмінність цих двох інструментів, вони є невід'ємними частинами менеджменту безперервності бізнесу та процедурно перетинаються. У цьому плані їх зручно розглянути за допомогою моделі менеджменту PDCA (Plan-Do-Check-Act) [21-23], основні завдання якої представлені на рис. 3.

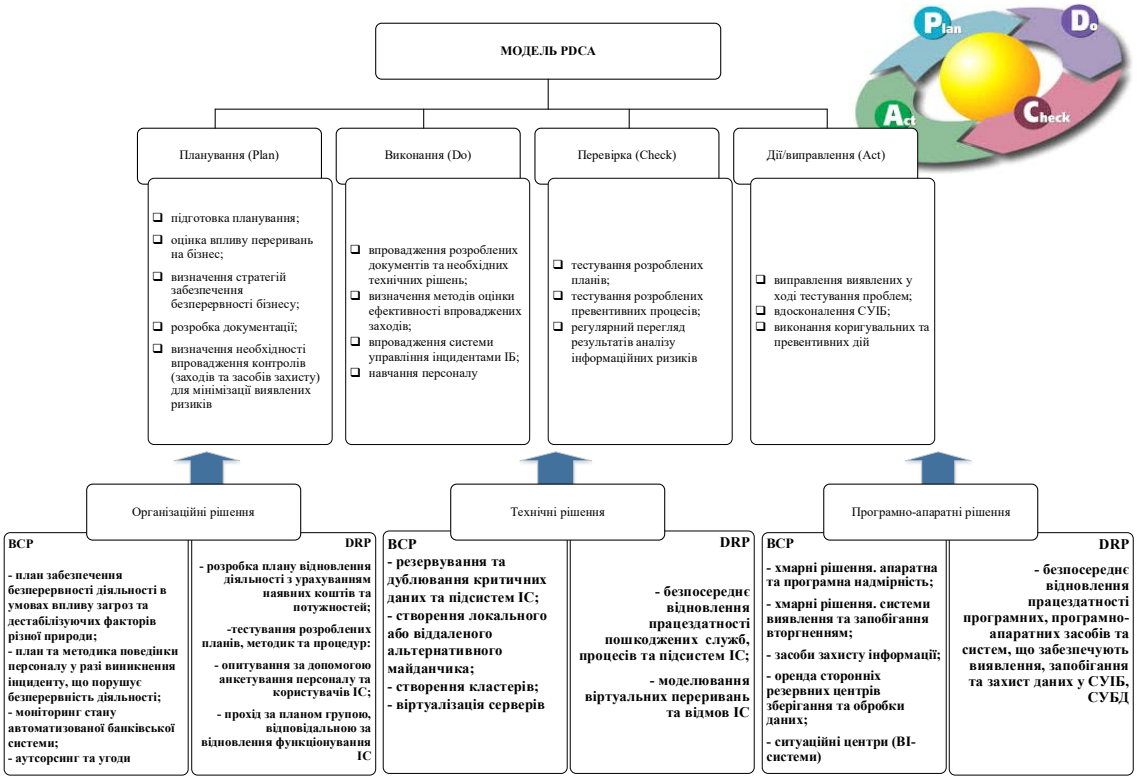


**Рис. 3.** Основні завдання та рішення забезпечення безперервності на етапах моделі менеджменту PDCA

Таким чином, запропоновані рішення мають свою вартість, сумісність, складність реалізації, час розгортання та ефективність, і можуть застосовуватися як окремо, так і у вигляді комплексу заходів, що реалізуються до, під час та/або після інциденту, що спричинив порушення безперервності функціонування автоматизованої банківської системи та діяльності ОБС.

Оцінка впливу переривань на бізнес (BIA) є ключовою темою безперервності бізнесу та полягає у функціональному аналізі того, як переривання вплинуть на діяльність організації.

До завдань BIA відносять [19,20,23]:

визначення цінності кожного бізнес-процесу;

ідентифікацію та ранжування переривань кожного бізнес-процесу;

пріоритизацію бізнес-процесів;

оцінку ресурсів забезпечення безперервності бізнес-процесів.

Підсумковим результатом BIA є вибір стратегій управління безперервністю бізнесу.

При визначенні цінності бізнес-процесів для інформаційних систем можуть бути зафіксовані значення ряду технічних показників [18,24], зв'язок між якими представлено на рис. 4:

MTPD (Maximum Tolerable Period of Disruption, максимально прийнятний період переривання бізнесу) – період часу, після якого несприятливі

наслідки, що виникли внаслідок переривання бізнесу, стають неприйнятними;

RTO (Recovery Time Objective, цільовий час відновлення) – період часу після переривання, протягом якого повинен бути відновлений мінімальний рівень діяльності організації, а також систем, що його підтримують, прикладних програм та функцій. Вважається, що: RTO <MTPD;

RPO (Recovery Point Objective, цільова точка відновлення) - період часу, за який повинні бути відновлені дані після переривання;

MAO (Maximum Allowable Outage, максимально допустимий час простою) – період часу, після якого існує ризик остаточного припинення діяльності ОБС, якщо надання сервісів, даних, бізнес-процесів та/або послуг не буде відновлено;

TOF (поточний час простою) – період часу, протягом якого діяльність була перервана внаслідок відмови ІС або її компонентів, недоступності сервісів та даних, у прийнятному для підприємства випадку має бути менше максимально допустимого часу простою. Вважається, що TOF≤MAO;

SDO (Service Delivery Objective, цільова доступність сервісу) – показує рівень доступності сервісу у певний час;

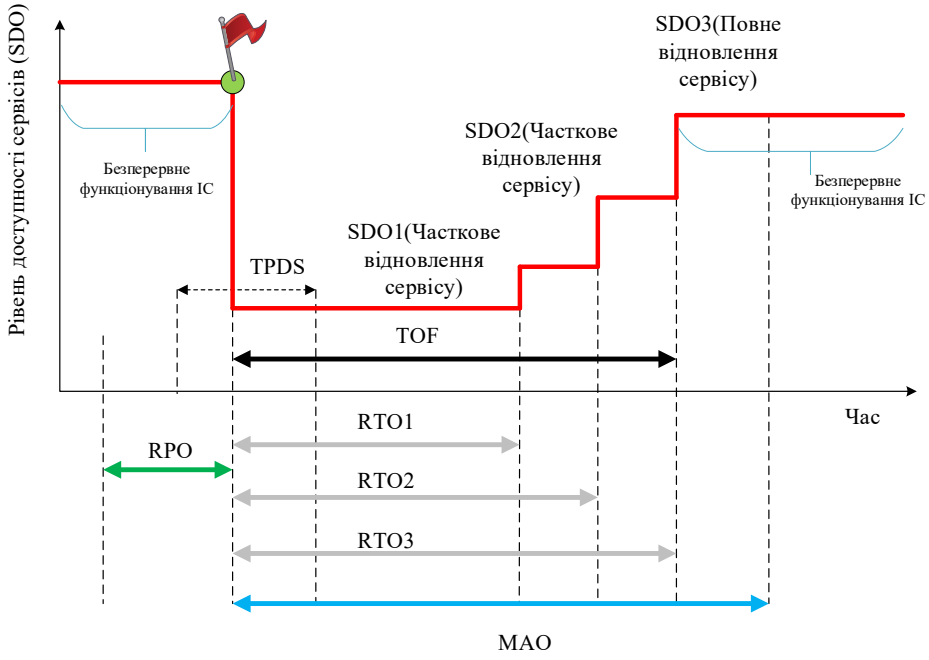


**Рис. 4.** Визначення показників безперервності діяльності

TPDS – час планування та розгортання рішень забезпечення та відновлення безперервності діяльності, в ідеальному випадку рішення та плани мають бути розроблені та впроваджені до настання інциденту порушення безперервності, TPDS < RTO.

Аналіз рис. 4 показав, що зниження TOF необхідний комплексний підхід до вирішення завдань BCP і DRP. Впровадження превентивних заходів захисту від кіберзагроз, спрямованих на порушення безперервності, дозволить не тільки мінімізувати втрати даних банківської інформації в автоматизованих банківських системах, а й скоротити цільовий час відновлення даних.

Подібний ефект досягається за рахунок того, що плани та засоби забезпечення безперервності діяльності розробляються та розгортаються не під час відмови, а в період штатного функціонування автоматизованої банківської системи до реалізації загрози та виникнення лавинного ефекту. Це дозволяє відразу після настання інциденту скоординувати дії персоналу та почати відновлення або повністю уникнути простою та втрат за рахунок оперативного перемикання на резервний майданчик (рис. 5) [18,24].

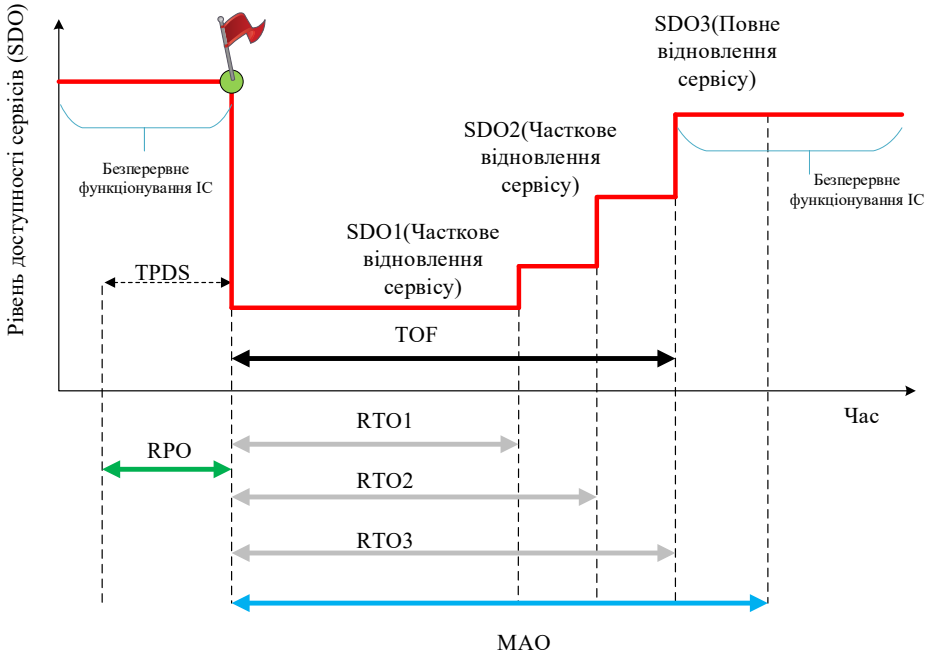


**Рис. 5.** Зниження часу відновлення функціонування TOF за рахунок застосування превентивних планів та заходів захисту

Таким чином, для забезпечення комплексного підходу безперервності бізнес-процесів ОБС пропонується використовувати дублювання автоматизованої банківської системи на основі концепції альтернативних майданчиків (майданчик у гарячому резерві (Hot Site), майданчик у теплому резерві (Warm Site), майданчик у холодному резерві (Cold Side) з використанням стратегій актуалізації даних – protection, періодична передача копій баз даних на альтернативні носії, зазвичай у пакетному режимі), віддалене журналування (remote journaling, періодична передача журналу виконаних транзакцій з основного майданчика на альтернативний), дистанційне віддзеркалення (remote mirroring, повне дублювання в реальному часі), що забезпечить необхідні показники цінності бізнес-процесів.

## 3. Висновки та перспективи подальшого розвитку

В результаті проведеного дослідження було сформовано цілісне уявлення про актуальність проблеми забезпечення безперервності бізнес-процесів в умовах зростання рівня кіберзагроз, особливо з боку суб'єктів, що здійснюють терористичну діяльність у кіберпросторі. Здійснений аналіз дозволив визначити ключові напрями протидії таким загрозам шляхом удосконалення методів оцінювання стійкості функціонування об'єктів критичної інфраструктури.

В результаті проведеого дослідження:

1) проаналізовано основні тенденції розвитку кібербезпеки в умовах досконалості засобів та способів ведення терористичних інформаційних атак на об'єкти критично важливих інфраструктур;

2) розглянуто основні завдання забезпечення безперервності бізнес-процесів на основі моделі ризику управління PDCA, показники оцінки забезпечення безперервності бізнес-процесів ОБС. Проаналізовано вплив обраних стратегій та рішень щодо забезпечення безперервності бізнес-процесів ОБС.

Проведений аналіз дозволяє зробити узагальнення щодо необхідності подальших досліджень щодо підвищення стійкості критичної інформаційної інфраструктури до кібертерористичних загроз. Зокрема, перспективним напрямом є розроблення інтегрованої моделі адаптивного реагування на кіберзагрози, що дозволить ефективно забезпечувати безперервність бізнес-процесів та мінімізувати вплив інцидентів на об'єкти критичної інфраструктури.

Можливі напрями наукового пошуку доцільно спрямувати на створення методології оцінки ефективності кіберзахисту в умовах зростаючої інтенсивності та складності загроз; розробку інтелектуальних систем підтримки прийняття рішень у сфері безперервності бізнесу під час кіберінцидентів; застосування агентного моделювання кіберзагроз з метою виявлення потенційних уразливостей в системах управління критично важливих об'єктів.

Дані напрями подальших досліджень послідовно розвивають тематику захисту інформаційної інфраструктури та сприяють удосконаленню засобів кібербезпеки в сучасному цифровому середовищі.

ЛІТЕРАТУРА


1. Грищук Р.В. (2016), Основи кібернетичної безпеки: монографія, Р.В. Грищук, Ю.Г. Даник; за заг. ред. Ю.Г. Данника, Житомир: ЖНАЕУ, 636 с.
2. Models of socio-cyber-physical systems security: monograph (2023), S. Yevseiev, Yu. Khokhlachova, S. Os- tapov, O. Laptiev and others, Kharkiv: PC TECHNOLOGY CENTER, 168 p.
3. Synergy of building cybersecurity systems: monograph (2021), S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others, Kharkiv: PC TECHNOLOGY CENTER, 188 p.
4. Modeling of security systems for critical infrastructure facilities: monograph (2022), S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others, Kharkiv: PC TECHNOLOGY CENTER, 196 p.
5. Діордіца І. В. (2016), Поняття і зміст кібертероризму, *Прикарпатський юридичний вісник,* Вип. 3 (12), С. 61–68.
6. Довгань О. Д., Доронін І. М. (2017), Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія: НАПрН України, НДІІП, К.: Видавничий дім «АртЕк», 107 с.
7. Почепцов Г. (2015), Сучасні інформаційні війни, Київ: Києво-Могилян. акад., 496 с.
8. Muqarrab A., Tasawar B. (2024), Making Sense of Cyber-Caliphate: A Transnational Movement in an era of hyper-globalization, *Pakistan Journal of Islamic Research*, Vol. 19, №. 1, pp. 123 – 138.
9. Голубєв В.О. (2020), Кібертероризм, як нова форма тероризму, URL: http://www.crimeresearch.org/library/Gol_tem3.ht.–10.04.0.
10. Бараненко Р. В. (2021), Кібератаки як одна з форм кібертероризму, *Вчені записки ТНУ імені В.І. Вернадського*, Серія: Технічні науки, Том 32 (71), Ч. 1, № 1, С. 45-50.
11. Банк Р.О. (2016), Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект, *Інформація і право*, № 1(16), С. 110-116.
12. Мельник Д.С. (2023), Кібертероризм: поняття, форми прояву, перспективні заходи протидії, *Вісник Харківського національного університету внутрішніх справ,* Харків, № 3(102), С. 144-158.
13. Мельник Д. С., Леонов Б.Д. (2024), Інформаційний тероризм як загроза національній інформаційній інфраструктурі, *Інформація і право*, №3(50), DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311667.
14. Малахов Г. Б. (2024), Використання кіберпростору як інструменту інформаційного тероризму, *Інформація і право*, №3(50), DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311671.
15. Kovalchuk T. I., Korystin O. Y., Sviridyuk N. P. (2019), Hybrid threats in the civil security sector in Ukraine, *Problems of Legality*, issue 147, pp. 163–175, doi: https:// doi.org/10.21564/2414-990x.147.180550.
16. Леоненко Г.П, Юдин А.Ю. (2013), Проблеми забезпечення інформаційної безпеки систем критично важливої інформаційної інфраструктури України, *Information Technology and Security*, № 1(3), С. 44-48.
17. Бурячок В.Л., Толюпа С.В., Семко В.В. та ін. (2016), Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби, Київ, ДУТ-КНУ, 178 с.
18. Кухарська Н., Полотай О. (2019), Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації, *Information Technology and Security*, Vol. 7, Iss. 2 (13), C.126-136, DOI 10.20535/2411-1031.2019.7.2.190555.
19. Ситайло У. В. (2024), Безперервність бізнесу в Україні: виклики та можливості в умовах війни, *Економіка та суспільство*, Випуск 62, URL: https://doi.org/10.32782/2524-0072/2024-62-22.
20. Дубецький О. (2023), Управління безперервністю бізнесу в кібербезпеці, URL: https://surli.cc/lrqtsp.
21. ISO/IEC 27031:2011 Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity, URL: http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374.
22. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements, URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.
23. Скіцько О., Ширшов Р. (2013), Система управління інформаційної безпеки як інструмент підвищення захищеності та ефективності об'єктів критичної інфраструктури, *International Science Journal of Engineering & Agriculture*, Vol. 2, No. 6. pp. 12-22, doi: 10.46299/j.isjea.20230206.02.
24. What Is the Difference Between RTO, RPO, and MTPD in BCP?, UniSense Advisory, URL: https://unisenseadvisory.com/.


REFERENCES


1. Hryshchuk R.V. (2016), Osnovy kibernetychnoi bezpeky: monohrafiia / R.V. Hryshchuk, Yu.H. Danyk; za zah. red. Yu.H. Dannyka, Zhytomyr: ZhNAEU, 636 s.
2. Models of socio-cyber-physical systems security: monograph (2023), S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others, Kharkiv: PC TECHNOLOGY CENTER, 168 p.
3. Synergy of building cybersecurity systems: monograph (2021), S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others, Kharkiv: PC TECHNOLOGY CENTER, 188 p.
4. Modeling of security systems for critical infrastructure facilities: monograph (2022), S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others, Kharkiv: PC TECHNOLOGY CENTER, 196 p.
5. Diorditsa I. V. (2016), Poniattia i zmist kiberteroryzmu, *Prykarpatskyi yurydychnyi visnyk*, Vyp. 3 (12), S. 61–68.
6. Dovhan O. D., Doronin I. M. (2017), Eskalatsiia kiberzahroz natsionalnym interesam Ukrainy ta pravovi aspekty kiberzakhystu: monohrafiia: NAPrN Ukrainy, NDIIP. K.: Vydavnychyi dim «ArtEk», 107 s.
7. Pocheptsov H. (2015), Suchasni informatsiini viiny, Kyiv: Kyievo-Mohylian. akad., 496 s.
8. Muqarrab A., Tasawar B. (2024), Making Sense of Cyber-Caliphate: A Transnational Movement in an era of hyper-globalization, *Pakistan Journal of Islamic Research*, Vol. 19, №. 1, pp. 123 – 138.
9. Holubiev V.O. (2020), Kiberteroryzm, yak nova forma teroryzmu, URL: http://www.crimeresearch.org/library/Gol_tem3.ht.–10.04.0.
10. Baranenko R. V. (2021), Kiberataky yak odna z form kiberteroryzmu, *Vcheni zapysky TNU imeni V.I. Vernadskoho*, Seriia: Tekhnichni nauky, Tom 32 (71), Ch. 1, № 1, S. 45-50.
11. Bank R.O. (2016), Informatsiinyi teroryzm yak zahroza natsionalnii bezpetsi Ukrainy: teoretyko-pravovyi aspekt, *Informatsiia i pravo*, № 1(16), S. 110-116.

12. Melnyk D.S. (2023), Kiberteroryzm: poniattia, formy proiavu, perspektyvni zakhody protydii, *Visnyk Kharkivskoho natsionalnoho universytetu vnutrishnikh sprav*, Kharkiv, № 3(102). S. 144-158.
13. Melnyk D. S., Leonov B.D. (2024), Informatsiinyi teroryzm yak zahroza natsionalnii informatsiinii infrastrukturi, *Informatsiia i pravo*, №3(50), DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311667.
14. Malakhov H. B. (2024), Vykorystannia kiberprostoru yak instrumentu informatsiinoho teroryzmu, *Informatsiia i pravo*, №3(50), DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311671.
15. Kovalchuk T. I., Korystin O. Y., Sviridyuk N. P.(2019), Hybrid threats in the civil security sector in Ukraine, *Problems of Legality*, issue 147, pp. 163–175, doi: https:// doi.org/10.21564/2414-990x.147.180550.
16. Leonenko H.P., Yudyn A.Iu. (2013), Problemy zabezpechennia informatsiinoi bezpeky system krytychno vazhlyvoi informatsiinoi infrastruktury Ukrainy, *Information Technology and Security,* № 1(3), S. 44-48.
17. Buriachok V.L., Toliupa S.V., Semko V.V. ta in. (2016), Informatsiinyi ta kiberprostory: problemy bezpeky, metody ta zasoby borotby, Kyiv, DUT-KNU, 178 s.
18. Kukharska N., Polotai O. (2019), Aspekty informatsiinoi bezpeky v upravlinni bezperervnistiu diialnosti orhanizatsii, *Information Technology and Security*, Vol. 7, Iss. 2 (13), C.126-136, DOI 10.20535/2411-1031.2019.7.2.190555.
19. Sytailo U. V. (2024), Bezperervnist biznesu v Ukraini: vyklyky ta mozhlyvosti v umovakh viiny, *Ekonomika ta suspilstvo*, Vypusk 62, URL: https://doi.org/10.32782/2524-0072/2024-62-22.
20. Dubetskyi O. (2023), Upravlinnia bezperervnistiu biznesu v kiberbezpetsi, URL: https://surli.cc/lrqtsp.
21. ISO/IEC 27031:2011 Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity, URL: http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374.
22. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements, URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534.
23. Skitsko O., Shyrshov R.(2013), Systema upravlinnia informatsiinoi bezpeky yak instrument pidvyshchennia zakhyshchenosti ta efektyvnosti obiektiv krytychnoi infrastruktury, *International Science Journal of Engineering & Agriculture*, Vol. 2, No. 6, pp. 12-22, doi: 10.46299/j.isjea.20230206.02.
24. What Is the Difference Between RTO, RPO, and MTPD in BCP?, UniSense Advisory, URL: https://unisenseadvisory.com/.

Received (Надійшла) 14.04.2025
Accepted for publication (Прийнята до друку) 05.05.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

**Король Ольга Григорівна** – кандидат технічних наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
**Olha Korol** – Candidate of Technical Sciences, Associate Professor, Associate Professor of Cyber Security Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: Olha.Korol@khpi.edu.ua; ORCID Author ID: https://orcid.org/0000-0002-8733-9984;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57190437459.

**Аксьонова Ірина Вікторівна** – кандидат економічних наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
**Iryna Aksonova** – Candidate of Economic Science, Associate Professor, Associate Professor of Cyber Security Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: ivaksyonova@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-2605-0455;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57206727489

**Севрюкова Єлизавета Олександрівна** – аспірант кафедри економіки підприємства та організації бізнесу, Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна;
**Yelyzaveta Sevriukova** – PhD student Department of Enterprise Economics and Business Organization, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine;
e-mail: elizavetasevryukova@ukr.net; ORCID Author ID: https://orcid.org/0000-0002-0757-490X
Scopus ID: https://id.elsevier.com/settings/redirect?code=xaA97O7kQqL9KGS_oS5KayF4fJIPqynH9TByHmrJ.

## DEVELOPMENT OF A METHOD FOR ASSESSING BUSINESS PROCESSES CONTINUITY IN CRITICAL INFRASTRUCTURE FACILITIES

O. Korol, I. Aksonova, Y. Sevriukova

**Abstract.** The **relevance** of the study is due to the growing dependence of critical infrastructure facilities on information technologies and the intensification of cyber threats, which pose significant risks to the continuity of business processes. Organizations of the banking sector are particularly vulnerable, for which even a short-term suspension of work can lead to significant financial and reputational losses. The **subject of the study** is approaches, strategies and indicators for assessing the level of ensuring the continuity of business processes in the conditions of cyber threats, as well as the impact of security factors on the effectiveness of the functioning of critical infrastructure facilities. The **purpose of the article** is to study approaches to ensuring the sustainable operation of business processes of banking sector organizations in the conditions of growing cyber threats by analyzing mechanisms for improving systems for preventing terrorist acts directed at critical infrastructure facilities. As a **result** of the study: the nature and means of implementing terrorist cyber threats to critical infrastructure facilities were analyzed; key strategies for ensuring business continuity are identified and relevant indicators for their assessment are determined; an approach to assessing the impact of strategic decisions on the level of continuity of business processes is proposed; a general structure of the method is developed that allows modeling and assessing the stability of the functioning of banking sector organizations in conditions of destabilizing factors. **Conclusion.** The study allows to increase the validity of management decisions regarding the choice of continuity strategies. The proposed approach can be used as a basis for creating methodological recommendations for managing cyber risks in critical sectors of the economy.

**Keywords:** cyberterrorism, cyberattack, critical infrastructure, business process continuity, banking sector security.