



DOI [10.28925/2663-4023.2020.10.4553](https://doi.org/10.28925/2663-4023.2020.10.4553)

УДК 65.011.56:004

**Андрейченко Андрій Вадимович**

доктор економічних наук, доцент,

Професор кафедри менеджменту та інновацій

Одеський національний університет імені І. І. Мечникова, Одеса, Україна

ORCID: 0000-0002-1854-9099

*Avandreichenko@gmail.com*

**Горбаченко Станіслав Анатолійович**

кандидат економічних наук, доцент,

Доцент кафедри менеджменту та інновацій

Одеський національний університет імені І. І. Мечникова, Одеса, Україна

ORCID: 0000-0001-8442-9581

*Stas\_gorbachenko@ukr.net*

**Дикий Олег Вікторович**

кандидат юридичних наук, доцент,

Декан факультету кібербезпеки та інформаційних технологій

Національний університет «Одеська юридична академія», Одеса, Україна

ORCID : 0000-0001-9659-9350

*Olegdykyj@gmail.com*

## ОСОБЛИВОСТІ УПРАВЛІННЯ ПРОЄКТАМИ У СФЕРІ КІБЕРЗАХИСТУ

**Анотація.** У статті проведено концептуальну оцінку існуючого визначення терміну «проект» та вдосконалено його управлінське тлумачення. Сформульовано основні сутнісні характеристики проекту, наведено відповідний категоріальний апарат, що дозволяє систематизувати проектну діяльність та адаптувати її під різні об'єкти застосування. Зокрема, зроблена спроба уточнити визначення проекту для сфери кібербезпеки та кіберзахисту. Визначено процеси, що впливають на проектну діяльність на рівні держави, регіонів та окремих підприємств. Доведено, незважаючи на те, що проблеми кіберзахисту поступово зміщуються на державний рівень в контексті національної безпеки, проектна діяльність в означеній сфері відбувається, насамперед, на рівні окремих суб'єктів господарювання. Здійснено наукову оцінку кіберпростору в якості середовища для проектної діяльності. Виокремлено такі особливості проектів у сфері кіберзахисту як підвищений рівень впливу з боку держави, складність стадії ініціації, критичне значення термінів реалізації, значна диференціація за бюджетом, необмежена кількість можливих учасників, високий рівень персоніфікації, складність у розрахунках показників ефективності. Визначено ключові завдання управління проектами в сфері кібербезпеки: формулювання основної мети проекту та ранжирування його цілей, визначення необхідних обсягів та джерел фінансування, оцінка проектних ризиків, підбір виконавців проектних робіт, складання графіку реалізації проекту, визначення потреби у ресурсах, забезпечення контролю тощо. Сформовано пропозиції щодо оптимізації процесів управління проектами в сфері кіберзахисту. Наголошено на перспективності використання послідовних методів управління проектами, за рахунок спрощеної комунікації із замовниками, можливістю чітко розділити процес впровадження систем кіберзахисту на певні етапи, а також впровадити на означених етапах ефективний механізм моніторингу та контролю.

**Ключові слова:** проект; кібербезпека; кіберзахист; бюджет; ефективність; управління проектами.



## 1. ВСТУП

**Постановка проблеми.** Сучасні вимоги до кібербезпеки передбачають застосування прогресивних інструментів, що базуються на всебічному впровадженні інновацій та дозволяють, на підставі оптимального поєднання інформаційних технологій та високої кваліфікації виконавців, проводити аналіз факторів зовнішнього та внутрішнього середовища, здійснювати сценарний аналіз розвитку ситуації, постійно коригувати системи протидії кіберзагрозам з огляду на технічні можливості, а також з високою ймовірністю прогнозувати загрози та розробляти відповідні заходи для мінімізації можливих втрат. Одним із таких дієвих інструментів є управління проектами. Адже в усьому світі проектний підхід вже довів свою здатність значно підвищувати результативність та ефективність управлінських рішень, в тому числі й у контексті впровадження систем кіберзахисту.

**Аналіз останніх досліджень і публікацій.** Дослідження діяльності з управління проектами знайшли своє відображення у великій кількості наукових праць Р. Арчибальда, В. Г. Воронкової, К. О. Глубоченко, О. Б. Марцінковської, А. В. Чернихівської та інших. Проте, слід зауважити, що означеним дослідженням здебільшого не притаманна галузева специфіка. І навіть у роботах присвячених специфіці управління ІТ - проектами не фігурує окремо напрям кібербезпеки. Відтак питання щодо особливості управління проектами у сфері кіберзахисту, як на державному рівні, так і для окремих суб'єктів господарювання, все ще потребують додаткового уточнення.

**Мета статті.** Метою статті є дослідження особливостей проектної діяльності та, зокрема, проектного менеджменту у сфері кіберзахисту.

## 2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Протягом тривалого періоду вітчизняна теорія та практика відносила до проектної діяльності лише науково-дослідну, конструкторську та архітектурно-будівельну, і лише в останні роки проектний підхід довів власну результативність для майже всіх видів діяльності, особливо в ІТ-сфері.

Р. Арчибальд запропонував розуміти під терміном «проект» комплекс зусиль, здійснюваних з метою отримання конкретних унікальних результатів в рамках відведеного часу і в межах затвердженого бюджету, який виділяється на оплату ресурсів, що використовуються або споживаються в ході проекту [1]. В цьому визначенні виявляються основні проектні характеристики: унікальність, обмеження у часі та обмеженість в ресурсах. Проте унікальність відноситься до результату, а не до сукупності дій, що було б більш коректним.

Подібне визначення проекту, як послідовності взаємопов'язаних подій, які відбуваються протягом встановленого періоду часу і спрямовані на досягнення неповторного, але в той самий час визначеного результату, надає Ф. Бегюлі [2, с. 40]. Проте в ньому відсутня ресурсна обмеженість, що є важливою проектною характеристикою.

Існуюча практика державного і регіонального управління використовує поняття «проект» як можливий варіант реалізації планів, законів, пропозицій, програм тощо [3]. Також інколи проекти характеризуються як конкретні завдання з визначеними вихідними даними й встановленими результатами (цілями), що обумовлюють спосіб його вирішення [4, с. 18]. Проте використання такого визначення є досить обмеженим і не розкриває всієї сутності проектної діяльності.



Розширене управлінське тлумачення передбачає розуміння проєкту як елементу, фрагмента, етапу у виконанні певних програм, самодостатнього управлінського рішення господарського, фінансового характеру. Тобто проєкт передбачає не пропозицію, що допускає зміни, альтернативи, уточнення, а конкретне завдання, обмежене визначеними рамками в просторі і в часі, рівнем фінансування тощо [5, с. 36]. В цьому визначенні відсутній такий важливий аспект як неповторність, адже заходи, які необхідно здійснити для реалізації проєкту, мають такий рівень інновацій, комплексності й структурованості, який дозволяє відрізнити як один проєкт від іншого, так і проєкт від програми та плану.

В контексті кіберзахисту та кібербезпеки «проєкт» – це комплекс взаємопов'язаних та неповторних робіт, які відбуваються в умовах обмежень в часі та ресурсах і спрямовуються на досягнення визначеного результату. Він завжди спрямований на досягнення конкретної мети, задоволення певної потреби. Таке спрямування припускає бажаний вимірний результат, якого можна досягнути за визначений строк. Тому цілі проєкту мають бути чітко сформульованими, вимірюваними, обмеження – заданими, а встановлені вимоги – здійснюваними.

З огляду на вищевказане можна стверджувати, що найважливішими складовими сучасних тлумачень визначення категорії «проєкт» є обов'язковий елемент новизни, а також безпосередня орієнтація на результативність заходів в умовах певних обмежень у часі та ресурсах. Тобто однією із вагомих характеристик будь-якого проєкту є його інноваційна складова. Деякі науковці навіть наполягають на тому, що в основі кожного проєкту повинна бути певна унікальність чи неповторність, інші виділяють інноваційні проєкти у окрему категорію. Ідентифікаторами при цьому виступають базисна інновація, сформовані мета та завдання, комплекс проєктних заходів, система виконання та контролю за реалізацією означених заходів, показники ефективності та результативності проєкту.

Ядром інноваційної проєктної діяльності в сучасному світі виступає ІТ-сфера. А проблеми кібератак, кількість яких постійно зростає, а способи змінюються та удосконалюються, спровокували підвищену увагу до проєктів кіберзахисту та кібербезпеки. Серед чинників, що здійснюють найбільший вплив на проєктну діяльність в означених сферах можна виокремити наступні.

1. Підвищений рівень впливу з боку держави. Питання інформаційної та кібербезпеки наразі набули національного значення і держава, в процесі їхнього вирішення виконує відразу декілька функцій. По-перше держава встановлює стандарти національної безпеки у кіберпросторі. Згідно вітчизняного законодавства [6] основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. Паралельно із цим у світовому масштабі відбувається посилення контролю з боку правоохоронних органів за контентом національного інформаційного простору, за мережевим трафіком, засобами доступу до всесвітньої мережі. Зазначена тенденція разом із можливістю зменшення рівня анонімності у всесвітній мережі (із введенням «Інтернет-паспорту» для користувачів) свідчить, що панівний до останнього часу неоліберальний підхід до розуміння мережі Інтернет (так звана «Каліфорнійська ідеологія») зазнає кардинальних змін. Відбувається поступовий перехід до «технореалізму», зі сприйняттям ІТ як «технологій подвійного призначення» та ключовою роллю держави у розвитку мережі Інтернет [7].



По-друге, держава виступає як замовник проєктів кіберзахисту, забезпечує їхнє фінансування за власні кошти та залучає кошти сторонніх інвесторів, укладає угоди щодо реалізації проєктів та керує процесом взаємодії між їхніми учасниками. Важливість означеної діяльності підтверджують, зокрема події 2017 року, коли вірус «Ransom: Win32/Petya» атакував приватний і державний сектори економіки України, зокрема банки, аеропорти, державну залізничну компанію, телекомпанії, телекомунікаційні компанії, великі мережеві супермаркети, енергетичні компанії, державні фіскальні служби, органи державної влади і місцевого самоврядування.

По-третє, держава постає ініціатором процесів державно-приватної взаємодії. Зокрема, в рамках означених процесів можливе створення для громадян, представників промисловості та бізнесу консультаційних пунктів по допомозі у своєчасному виявленні, попередженні та нейтралізації кіберзагроз, а при необхідності консолідації зусиль у розслідуванні їх. Для створення таких центрів необхідно залучати волонтерські організації як українські, так і закордонні, що буде сприяти покращенню міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, та невідворотності покарання за вчинення кіберзлочинів [8, с. 19].

2. Складність стадії ініціації. Процес прийняття управлінських рішень для більшості проєктів в ІТ-сфері є набагато складнішим, ніж в інших сферах національної економіки. Це, насамперед, пов'язано з необхідністю формування технічного завдання, проведення аудиту бізнес - процесів, інтерв'ювання персоналу, придбання додаткових технічних засобів та програмних продуктів тощо. Крім того для проєктів в сфері кібербезпеки необхідне обґрунтування економічної доцільності та ефективності проєктів з огляду на можливі втрати від кіберзагроз, які взагалі не завжди можливо виміряти кількісно. З іншого боку в основу більшості проєктів в сфері кібербезпеки завжди можна покласти готове програмне рішення та адаптувати його до діяльності підприємства чи організації.

3. Критичне значення термінів реалізації проєкту. Для більшості проєктів саме часові обмеження вважаються найкритичнішими, в тому числі й у ІТ-сфері, де технології дуже швидко морально застарівають. З іншого боку, майже усі проєкти кібербезпеки потребують узгодження на різних рівнях керівництва. Тобто терміни виконання проєкту можуть суттєво затягнутися і дуже ймовірними наслідками при цьому є перевитрата ресурсів та/або недостатньо висока якість робіт (в цьому сенсі дуже допомагає вірно складений бриф). У більшості методів управління проєктами основний акцент робиться на календарному плануванні робіт і контролі за дотриманням графіка. Проте це досить складно зробити в умовах прямої залежності від зовнішніх неконтрольованих чинників.

4. Значна диференціація за бюджетом. Без попереднього аудиту бюджет проєктів кібербезпеки визначити майже неможливо. Наприклад, захистити електронні скриньки працівників можна безкоштовно. Інші проблеми вирішуються за допомогою використання ліцензійного «Windows» який автоматично оновлюється. В той самий час при наявності зовнішніх загроз може з'явитися потреба у спеціальному софті, фахівцях і значних проєктних витратах. Отже важливо від самого початку ідентифікувати основні загрози та ризики у кіберпросторі. І ніхто краще за керівництво конкретного підприємства чи організації не знає, які дані потрібно захистити, хто є основними конкурентами, які в них технологічні можливості і що може бути джерелом та об'єктом втручання.



5. Необмежена кількість можливих учасників проєктів. За своєю сутністю проєкти в сфері кібербезпеки є дуже різноманітними: деякі з них навіть не потребують складних технологічних рішень і спрямовуються на комунікацію із персоналом щодо обережності у кіберпросторі, а для реалізації інших залучають сторонніх підрядників, в тому числі й на аутсорсінг. Насамперед це стосується проєктів захисту від зовнішніх кіберзагроз учасники яких можуть знаходитися в різних країнах світу. Крім того для масштабних проєктів, на кшталт протидії хакерським атакам, які можуть змінювати результати виборів, залучається не тільки комерційний сектор, а й представники наукової спільноти, органів державної та місцевої влади тощо.

6. Високий рівень персоніфікації. Особливо це помітно у сегменті кібербезпеки підприємницьких структур, де унікальними є і клієнтські запити, і реальні та ментальні загрози, і запропоновані рішення. При чому клієнт може обирати або готове рішення (де існує величезний пул пропозицій) або індивідуальну розробку «під ключ».

7. Складність у розрахунках показників ефективності. Адже в основі методології оцінки усіх видів економічної ефективності лежить порівняння фінансових результатів від реалізації проєкту із фінансовими витратами на його розробку та реалізацію. Для більшості проєктів в якості основного вимірювача ефективності використовують показник чистого приведеного прибутку (Net present value, NPV), який характеризує загальний абсолютний результат інвестиційної діяльності. Коли потік надходжень характеризується розмірами  $R(t) = B(t) - C(t)$  і означені величини можуть бути як позитивними, так і негативними, то, за умови, що ставка дисконтування дорівнює  $i$ , можна отримати наступне рівняння:

$$NPV = \sum_{t=1}^n \frac{B(t) - C(t)}{(1+i)^t} = \sum_{t=1}^n \frac{R(t)}{(1+i)^t} = \sum_{t=1}^n R(t)V^t \quad (1)$$

Де  $Rt$  - розмір учасника потоку платежів;

$V$  - дисконтний множник за ставкою.

В результаті розрахунків, той інвестиційний проєкт, для якого чистий приведений дохід є негативним або дорівнює нулю, відхиляється, оскільки він не принесе додаткових доходів на вкладений капітал. Серед альтернативних проєктів для реалізації приймається той, для якого показник чистого приведеного прибутку є найвищим. Проте у сфері кібербезпеки не завжди існує пропорційний зв'язок між проєктним бюджетом та збільшенням прибутку.

Ще складніше ситуація із соціальною ефективністю проєктів з кібербезпеки, яка має проявлятися в можливості досягнення позитивних змін в організації заходів з точки зору умов діяльності персоналу. Адже деякі заходи спрямовані на кіберзахист якраз певним чином ускладнюють діяльність персоналу, потребують додаткових витрат часу та можуть змінити атмосферу в колективі.

В цьому сенсі ключового значення набуває ефективне управління проєктами. У загальному розумінні діяльність із управління проєктами вивчає теоретико-методологічні засади та формулює практичні рекомендації щодо планування, підготовки, програмування та впровадження проєктних рішень [9, с. 85]. З практичного погляду управління проєктами виступає як певний інструмент в для керівництва або управлінських команд, який дозволяє забезпечити максимальну прозорість окремих стадій, етапів, дій, визначити часові та фінансові витрати на певні операції, встановити дедлайни, зафіксувати власне навантаження та навантаження колег тощо.



Основними завданнями при управлінні проектами в сфері кібербезпеки виступають: визначення основної мети проекту та її обґрунтування, структуризація та ранжирування цілей проекту, визначення необхідних обсягів та джерел фінансування, дослідження та врахування проектних ризиків, підбір виконавців проектних робіт. Підготовка та укладання контрактів, визначення термінів виконання проекту, складання графіку реалізації; визначення потреби у ресурсах (трудових, матеріальних та фінансових); складання кошторису та бюджетування проекту; забезпечення контролю та моніторингу проекту.

Серед методів управління проектами в сфері кібербезпеки, найчастіше використовують послідовні методи. Використання означених методів, по-перше, спрощує комунікації із замовниками (керівниками підприємств чи представниками органів державної влади), по-друге, дозволяє чітко розділити процес впровадження систем кіберзахисту на певні етапи і, по-третє, дає можливість побудувати ефективний механізм моніторингу та контролю за реалізацією проекту.

Зокрема, метод водоспаду передбачає, що певне завдання повинне бути завершене до початку наступного, що створює зв'язок у послідовності елементів на шляху до результату. Він повністю підходить для проектів у сфері кіберзахисту, адже кожен крок спланований і має своє місце в правильній послідовності. З іншого боку зміни в потребах або пріоритетах клієнтів відразу порушують послідовність завдань, що спричиняє проблеми в управлінні.

Метод критичного шляху ґрунтується на концепції існування деяких завдань, які не можна розпочати, поки попередні не будуть завершені. Критичний шлях і позначає послідовність цих завдань. В свою чергу виявлення та зосередження уваги на цьому критичному шляху дає змогу керівникам проектів визначити пріоритети і розподіляти ресурси, щоб сконцентруватися на найважливіших процесах та перепланувати будь-які пріоритетні завдання, які можуть вплинути на продуктивність команди. Таким чином, якщо певні зміни повинні бути внесені в графік проекту, процес роботи команди можна оптимізувати без затримки кінцевих результатів [10, с. 104].

І, нарешті, ланцюговий метод ставить основний акцент на ресурси, необхідні для виконання завдань проекту. Після визначення послідовності найважливіших завдань відбувається резервування ресурсів разом із створенням часового буферу навколо цих завдань у розкладі проекту, для вкладання у необхідні терміни.

### **3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ**

Серед причин, що ускладнюють процеси інноваційного розвитку вітчизняних суб'єктів господарювання фігурують такі чинники як недостатній рівень інформатизації та автоматизації, моральна застарілість технологій, малоефективна діяльність з формування та аналізу баз даних. Зменшити негативний вплив означених чинників менеджмент намагається за рахунок проектної діяльності, насамперед, у вигляді інноваційних проектів в сфері інформаційних технологій. Однак, означені проекти виступають не тільки важелем розвитку, а й джерелом кіберзагроз. Відтак, поступово кіберзахист займає свою нішу у проектній діяльності. Проекти в сфері кіберзахисту характеризуються певними особливостями (на кшталт, підвищеного залучення органів державної влади, складної стадії ініціації, критичної важливості дотримання термінів реалізації, значної диференціації бюджетів, високого рівня персоніфікації, складності у розрахунках показників ефективності) і, одночасно, потребують специфічних управлінських підходів.



## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Арчибальд Р. Управление высокотехнологичными программами и проектами. URL: <http://pmwebinars.ru/wp-content/uploads/2013/07/Rassel-D.-Archibald-Upravlenie-vyisokotekhnologichnyimi-programmami-i-proektami.pdf>
- [2] Бэбьюли Ф. Управление проектом / Пер. С англ. В. Петрашек. Москва: ФАИР-ПРЕСС, 2002. 208 с.
- [3] Чернихівська А. В. Переваги застосування проектного менеджменту у сфері регіонального управління. URL: <http://www.sedu.com.ua/archive/34/pdf/10.pdf>
- [4] Воронкова В. Г., Романенко Т. П., Андрюкайтене Р. Концепція розвитку проектно-орієнтованого бізнесу в умовах цифрової трансформації до SMART-суспільства. *Гуманітарний вісник Запорізької державної інженерної академії*. 2016. Вип. 67 (2016). С. 13 - 27.
- [5] Макух Я. Д. Термінологічні рівні поняття «проект». *Глобалізація та управління проектами у XXI столітті: матеріали наук.-практ. Конф. (Львів, 9-10 жовт. 2003 р.)*, 2003. - С. 35-37.
- [6] Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII, редакція від 03.07.2020. Р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
- [7] Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка. Національний інститут стратегічних досліджень. URL: <http://old2.niss.gov.ua/articles/294/>
- [8] Браїловський М. М., Хорошко В. О. Особливості кібербезпеки на підприємствах України в сучасних умовах. *Безпека соціально-економічних процесів в кіберпросторі : матеріали Всеукр. Наук.-практ. Конф. (Київ, 27 берез. 2019 р.)*. 2019. С. 18-20.
- [9] Глубоченко К. О. Особливості застосування технологій проектного менеджменту в галузі місцевого самоврядування. *Наукові праці. Державне управління*. 2013. Випуск 202. Том 214. С. 84-87.
- [10] Марцінковська О. Б. Сучасні підходи до управління командами в контексті реалізації проекту. *Регіональні аспекти розвитку продуктивних сил України*. 2016. Вип. 21. С. 102-108.

**Andrii V. Andreichenko**

Doctor of Economics, Associate Professor,  
Professor at the Department of Management and Innovations,  
Odessa I. I. Mechnikov National University, Odessa, Ukraine  
ORCID: 0000-0002-1854-9099  
Avandreichenko@gmail.com

**Stanislav A. Horbachenko**

Phd in Economics, Associate Professor,  
Associate Professor at the Department of Management and Innovations,  
Odessa I. I. Mechnikov National University, Odessa, Ukraine  
ORCID: 0000-0001-8442-9581  
Stas\_gorbachenko@ukr.net

**Oleh V. Dykyi**

Phd in Law, Associate Professor,  
Dean of the Faculty of Cyber Security and Information Technology  
National University «Odessa Law Academy», Odessa, Ukraine  
ORCID: 0000-0001-9659-9350  
Olegdykyj@gmail.com

**PECULIARITIES OF PROJECT MANAGEMENT IN CYBER DEFENSE**

**Abstract.** The article provides a conceptual assessment of the existing definition of the term "project" and improved its management interpretation. The main essential characteristics of the project are formulated, the corresponding categorical device is given, which allows to systematize the project activity and adapt it to different objects of the application. In particular, an attempt was made to clarify the definition of the project in cybersecurity and cyberdefense. The processes influencing project activity at the level of the state, regions, and separate enterprises are defined. It is proved that although the problems of cybersecurity are gradually shifting to the state level in the context of national security, project activities in this area occur primarily at the level of the individual business. The peculiarities of cybersecurity projects such as increased level of state influence, the complexity of the initiation stage, critical implementation deadlines, significant budget differentiation, unlimited number of possible participants, high level of personalization, difficulty in calculating efficiency indicators are highlighted. The key tasks of project management in cybersecurity are defined: formulation of the main goal of the project and ranking of its goals, determination of necessary volumes and sources of financing, assessment of project risks, selection of project executors, scheduling of project implementation, resource requirements, control, etc. Proposals for optimizing project management processes in the field of cybersecurity have been formed. Emphasis is placed on the prospects of using consistent project management methods, due to simplified communication with customers, the ability to divide the process of implementing cybersecurity systems into certain stages, as well as to introduce an effective monitoring and control mechanism at these stages.

**Keywords:** project; cybersecurity; cyber defense; budget; efficiency; project management

**REFERENCES**

- [1] Archibald R. Management of high-tech programs and projects. URL: <http://pmwebinars.ru/wp-content/uploads/2013/07/Rassel-D.-Archibald-Upravlenie-vyisokotekhnologichnyimi-programmami-i-proektami.pdf>
- [2] Baguli F. Project Management / Transl. From English. V. Petrashek. Moscow: FAIR-PRESS, 2002. 208 p.
- [3] Chernykhivska A. V. Advantages of project management application in regional management. URL: <http://www.sedu.com.ua/archive/34/pdf/10.pdf>





- [4] Voronkova V. G., Romanenko T. P., Andryukaitene R. The concept of development of project-oriented business in the conditions of digital transformation to SMART-society. *Humanitarian Bulletin of the Zaporizhia State Engineering Academy*. 2016. Vol. 67 (2016), pp. 13 - 27.
- [5] Makukh J. D. Terminological levels of the concept of "project". *Globalization and project management in the XXI century: materials of scientific practice. Conf.*, (Lviv, October 9-10, 2003), 2003, pp. 35-37.
- [6] On the basic principles of cybersecurity of Ukraine: Law of Ukraine № 2163-VIII, edition of 03.07.2020. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
- [7] Current trends in cybersecurity policy: conclusions for Ukraine. Analytical note. National Institute for Strategic Studies. URL: <http://old2.niss.gov.ua/articles/294/>
- [8] Brailovsky M. M., Khoroshko V. O. Features of cybersecurity at the enterprises of Ukraine in modern conditions. *Security of socio-economic processes in cyberspace: materials of All-Ukrainian scientific-practical conf.* (Kyiv, March 27, 2019). 2019, pp. 18-20.
- [9] Glubochenko K. O. Peculiarities of application of project management technologies in the field of local self-government. *Scientific works. Governance*. 2013. Issue 202, vol. 214, pp. 84-87.
- [10] Martsinkovska O. B. Modern approaches to team management in the context of project implementation. *Regional aspects of development of productive forces of Ukraine*. 2016. Issue 21, pp. 102-108.

