УДК 331(075.8)

Гоч Павло Віталійович
(аспірант ПВНЗ «Європейський університет»)
ORCID ID 0009-0005-4472-3571

Чаплик Тарас Володимирович
(аспірант ПВНЗ «Європейський університет»)
ORCID ID 0009-0005-8247-8669

ІНТЕГРАЦІЯ ІНТЕЛЕКТУАЛЬНОГО КАПІТАЛУ В СТРАТЕГІЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Анотація. *У статті досліджено інтеграцію інтелектуального капіталу у стратегію забезпечення інформаційної безпеки підприємств. Висвітлено взаємозв'язки між людським, організаційним та клієнтським капіталом і компонентами інформаційної безпеки. Розглянуто інноваційні підходи до захисту інформації, які базуються на знаннях і компетенціях персоналу, а також сучасні технології, що підтримують управління інтелектуальним капіталом. Надано практичні рекомендації для підприємств щодо вдосконалення системи інформаційної безпеки в умовах цифровізації та зростання кіберзагроз.*

Ключові слова: *інтелектуальний капітал, інформаційна безпека, кіберзагрози, людський капітал, корпоративна культура, інноваційні підходи, цифровізація.*

Постановка проблеми. З розвитком цифрових технологій підприємства стикаються зі зростаючими викликами у сфері інформаційної безпеки. Уразливість до кіберзагроз стає однією з головних проблем, яка підриває як функціонування бізнесу, так і довіру клієнтів. У цьому контексті інтеграція інтелектуального капіталу у стратегію інформаційної безпеки набуває стратегічного значення. Знання, компетенції та досвід персоналу, разом із ефективним використанням організаційних і клієнтських активів, можуть забезпечити комплексний підхід до захисту інформаційних ресурсів підприємства.

Аналіз останніх досліджень і публікацій. Дослідження у сфері інформаційної безпеки активно розвиваються. Зокрема, науковці звертають увагу на вплив людського фактора та організаційних інновацій на стійкість до кіберзагроз. У роботах науковців Сміта Дж., Брауна Л. підкреслюється значення навчання персоналу для запобігання атакам, заснованим на соціальній інженерії [5]. Науковці Лю Х., Чжао Х. акцентують на важливості впровадження автоматизованих систем моніторингу загроз на основі штучного інтелекту [4]. Водночас питання комплексної інтеграції інтелектуального капіталу в стратегію інформаційної безпеки залишаються недостатньо дослідженими, що потребує подальшого аналізу.

Мета статті. Метою статті є вивчення ролі інтелектуального капіталу у забезпеченні інформаційної безпеки підприємств, визначення інноваційних підходів до інтеграції знань і компетенцій у системи захисту інформації, а також розробка практичних рекомендацій для вдосконалення стратегій управління інформаційними активами.

Виклад основного матеріалу дослідження. Інтелектуальний капітал є однією з ключових складових сучасного підприємства, яка визначає його конкурентоспроможність у динамічному та інформаційно насиченому середовищі. Це нематеріальний актив, який охоплює знання, компетенції, інновації та відносини, що забезпечують створення доданої

вартості. У структурі інтелектуального капіталу традиційно виділяють три основні компоненти: людський, організаційний та клієнтський капітал [6].

Людський капітал є основою інтелектуального капіталу підприємства. Він охоплює знання, навички, досвід та креативний потенціал працівників, які формують здатність організації до інновацій та адаптації. Людський капітал включає як професійну компетентність персоналу, так і його здатність до навчання та саморозвитку. В умовах інформаційної економіки людський капітал стає визначальним фактором для впровадження інноваційних рішень, зокрема у сфері інформаційної безпеки. Організаційний капітал включає нематеріальні активи, пов'язані зі структурою, процесами та системами підприємства. Це корпоративна культура, внутрішні регламенти, патенти, бази даних, системи управління знаннями, а також репутація компанії. Організаційний капітал є фундаментом для ефективного використання людського капіталу, створення інновацій та забезпечення інформаційної безпеки. Стабільні процеси та сильна корпоративна культура сприяють підвищенню рівня захисту інформаційних ресурсів. Клієнтський капітал відображає відносини підприємства з його клієнтами, партнерами та іншими зацікавленими сторонами. Це включає лояльність клієнтів, ділову репутацію, брендову силу, контракти та інші нематеріальні активи, що формуються на ринку[7]. У контексті інформаційної безпеки клієнтський капітал відіграє важливу роль у підтримці довіри до компанії, адже рівень захисту даних клієнтів безпосередньо впливає на її репутацію. Таким чином, інтелектуальний капітал є цілісною системою, що інтегрує людський, організаційний та клієнтський капітал. Його ефективне управління дозволяє підприємству досягати конкурентних переваг, створювати інновації та забезпечувати високий рівень інформаційної безпеки. Це підкреслює важливість синергії між компонентами інтелектуального капіталу в умовах сучасної економіки знань [4].

Знання, досвід і компетенції персоналу відіграють ключову роль у забезпеченні інформаційної безпеки підприємства. У сучасних умовах, коли цифровізація та автоматизація процесів стають невід'ємними складовими діяльності організацій, саме людський капітал стає центральним елементом у формуванні стійкої системи захисту інформаційних ресурсів. Знання персоналу включають теоретичні та практичні аспекти роботи з інформаційними системами, знання принципів кібербезпеки, основних методів виявлення та запобігання кіберзагрозам. Працівники, які володіють глибокими знаннями у сфері інформаційних технологій та сучасних методів захисту даних, здатні не лише ефективно реагувати на загрози, але й прогнозувати потенційні ризики, що створює основу для превентивної безпеки. Досвід є важливим доповненням до знань, адже він дозволяє персоналу оперативно діяти в нестандартних чи кризових ситуаціях. Працівники, які вже стикалися з кіберінцидентами, здатні швидше адаптуватися до нових викликів та впроваджувати більш ефективні рішення. Крім того, досвід дає змогу ідентифікувати слабкі місця в системах безпеки та вдосконалювати їх [8].

Компетенції персоналу охоплюють ширший спектр навичок, необхідних для забезпечення інформаційної безпеки. Це не лише технічні вміння, як-от налаштування захисних програмних рішень чи роботи з системами моніторингу, але й організаційні та комунікаційні здібності. Наприклад, працівники повинні вміти співпрацювати між собою, обмінюватися інформацією про потенційні загрози, навчати нових членів команди та працювати в умовах динамічних змін. Крім того, рівень обізнаності працівників про загрози та основні принципи безпеки визначає ефективність захисту даних від людського фактора, який є однією з головних причин порушення інформаційної безпеки. Регулярні тренінги, навчання та сертифікація персоналу дозволяють мінімізувати ризик ненавмисних дій, таких як відкриття шкідливих електронних листів чи недотримання політик доступу до даних [6].

Узагальнюючи, знання, досвід і компетенції персоналу формують фундамент для ефективної системи інформаційної безпеки. Інвестиції в розвиток людського капіталу стають необхідною умовою для захисту інформаційних ресурсів та підтримки довіри клієнтів і партнерів. Організації, які приділяють увагу підвищенню кваліфікації своїх співробітників, створюють не лише технічно оснащену, але й інтелектуально підготовлену систему захисту від сучасних кіберзагроз [1].

Знання, досвід та компетенції персоналу є ключовими складовими формування ефективної системи інформаційної безпеки на підприємстві. У сучасному світі, де інформаційні активи є критично важливими для забезпечення конкурентоспроможності, персонал стає першою лінією оборони проти внутрішніх та зовнішніх загроз. Знання персоналу у сфері інформаційної безпеки дозволяють усвідомити потенційні ризики та загрози, які можуть виникнути під час роботи з інформаційними системами. Це включає базове розуміння принципів кібербезпеки, таких як управління паролями, захист даних, правила доступу до інформації та безпечне використання мережевих ресурсів. Високий рівень обізнаності співробітників щодо сучасних кіберзагроз, таких як фішинг, соціальна інженерія та вірусні атаки, є фундаментом для запобігання інцидентам безпеки [4]. Досвід співробітників забезпечує їхню здатність оперативно реагувати на загрози та знаходити ефективні рішення у нестандартних ситуаціях. Практичний досвід роботи з інформаційними системами, розуміння специфіки технологічних процесів підприємства, а також здатність передбачати можливі вразливості значно знижують ризики несанкціонованого доступу чи втрати даних. Досвідчені співробітники також можуть виявляти слабкі місця в існуючих протоколах безпеки та ініціювати їх вдосконалення [5].

Компетенції персоналу, що включають технічні, організаційні та комунікаційні навички, є важливим чинником для забезпечення комплексного підходу до інформаційної безпеки. Наприклад, технічні компетенції дозволяють співробітникам налаштовувати та обслуговувати засоби захисту інформації, такі як антивірусні програми, системи шифрування даних, фаєрволи та інші технічні інструменти. Організаційні компетенції сприяють впровадженню політик і процедур безпеки, включаючи розробку планів дій на випадок надзвичайних ситуацій. Комунікаційні навички важливі для навчання та взаємодії з іншими співробітниками, щоб створити культуру інформаційної безпеки на всіх рівнях організації. Таким чином, знання, досвід та компетенції персоналу є невід'ємною складовою системи інформаційної безпеки підприємства. Без їх належного рівня навіть найдосконаліші технічні засоби захисту не зможуть гарантувати повного захисту інформаційних активів. Інвестиції в навчання, підвищення кваліфікації та розвиток компетенцій співробітників є стратегічним рішенням, що забезпечує довгострокову стійкість підприємства до сучасних загроз [8].

Інтелектуальний капітал є невід'ємною частиною сучасного підприємства, який відіграє важливу роль у формуванні ефективної системи інформаційної безпеки. Його структура включає людський, організаційний та клієнтський капітал, кожен із яких робить свій внесок у забезпечення захисту інформаційних активів підприємства [6]. Інтелектуальний капітал охоплює нематеріальні активи, що формують знання, досвід та організаційну інфраструктуру підприємства. У контексті інформаційної безпеки його структура включає [7]:

1. Людський капітал: знання, досвід та компетенції працівників, які забезпечують здатність до ідентифікації, запобігання та реагування на загрози.
2. Організаційний капітал: системи управління, політики безпеки, інновації, корпоративна культура, а також інформаційні технології, що сприяють побудові захищеного середовища.
3. Клієнтський капітал: довіра клієнтів, контракти та інші взаємозв'язки, які формують репутацію компанії як захисника даних.

Роль людського капіталу у забезпеченні інформаційної безпеки є фундаментальною. Працівники з відповідними знаннями та досвідом здатні ідентифікувати потенційні ризики та вживати превентивних заходів. Компетенції персоналу включають не лише технічні навички, але й організаційні та комунікаційні якості, які сприяють формуванню безпечного інформаційного середовища. Організаційні інновації, такі як розробка автоматизованих систем моніторингу загроз, впровадження стандартів кібербезпеки та інтеграція захисних технологій, сприяють побудові надійної системи інформаційного захисту. Корпоративна культура відіграє важливу роль у забезпеченні дотримання правил безпеки співробітниками. Формування культури інформаційної безпеки включає навчання персоналу, впровадження політик прозорості та стимулювання відповідальної поведінки [7]. Складові інтелектуального капіталу та їх роль в інформаційній безпеці представлена нами в таблиці 1.

Таблиця 1. **Складові інтелектуального капіталу та їх роль в інформаційній безпеці**

Складова інтелектуального капіталу	Опис	Роль в інформаційній безпеці
Людський капітал	Знання, досвід, компетенції працівників.	Ідентифікація загроз, розробка превентивних заходів, підвищення кваліфікації.
Організаційний капітал	Політики, процедури, корпоративна культура, інформаційні системи.	Створення структурованого підходу до управління безпекою, впровадження інновацій у захист інформаційних активів.
Клієнтський капітал	Довіра клієнтів, контракти, відносини з партнерами.	Підтримання довіри клієнтів через забезпечення безпеки їхніх даних, підвищення репутації підприємства.

Забезпечення інформаційної безпеки вимагає інтеграції всіх компонентів інтелектуального капіталу. Лише за умови їх синхронного розвитку підприємства можуть ефективно захищати свої інформаційні ресурси та формувати довіру з боку клієнтів і партнерів. У сучасних умовах глобалізації та активної цифровізації проблема інформаційної безпеки стає все більш актуальною для підприємств. З одного боку, цифрові технології відкривають нові можливості для розвитку бізнесу, з іншого — створюють численні ризики, які можуть поставити під загрозу як діяльність підприємства, так і його репутацію. Серед ключових викликів, з якими стикаються організації, виділяються кіберзлочинність, внутрішні загрози, технічні збої та недостатня обізнаність персоналу у сфері інформаційної безпеки [1].

Однією з найсерйозніших загроз для сучасного підприємства є кіберзлочинність (табл.2). Хакерські атаки, шкідливе програмне забезпечення, DDoS-атаки та фішинг стають дедалі більш поширеними явищами. Збитки, завдані кіберзлочинами, продовжують зростати, а їх масштаби охоплюють як фінансові втрати, так і репутаційні ризики. Водночас технологічна складність атак та їхня спрямованість на конфіденційні дані роблять підприємства вразливими, навіть за умови наявності захисних систем. Не менш важливим є питання внутрішніх загроз, пов'язаних із діяльністю працівників. Ненавмисні помилки, порушення встановлених політик безпеки або навіть зловмисні дії з боку персоналу можуть стати причиною значних втрат. Людський фактор залишається однією з найвразливіших ланок у системах безпеки, тому ефективне управління цим ризиком є обов’язковим для кожного підприємства [4].

Таблиця 2. **Основні загрози інформаційної безпеки підприємств у цифрову епоху**

Загроза	Опис	Наслідки
Кіберзлочинність	Хакерські атаки, шкідливе ПЗ, фішинг, DDoS-атаки.	Витік даних, фінансові втрати, репутаційні ризики.
Внутрішні загрози	Помилки співробітників, порушення політик безпеки, зловмисні дії.	Втрата конфіденційності, порушення роботи систем.
Технічні збої	Проблеми з апаратним чи програмним забезпеченням, відсутність резервування даних.	Зупинка бізнес-процесів, втрата даних.
Нестача знань персоналу	Недотримання правил кібергігієни, відсутність регулярного навчання.	Підвищення ризику атак, вразливості до соціальної інженерії.

Технічні збої також створюють серйозні виклики для інформаційної безпеки. Проблеми з апаратним або програмним забезпеченням, відсутність резервування даних або несвоєчасне оновлення систем можуть призвести до значних втрат або зупинки бізнес-процесів. Застарілі інформаційні системи та недостатній рівень моніторингу лише посилюють цю проблему.Особливе місце у формуванні інформаційної безпеки займає питання обізнаності персоналу. Співробітники, які не дотримуються базових правил кібергігієни, часто стають мішенню для атак. Фішинг, недотримання паролів, неналежний захист робочих пристроїв — усе це значно підвищує вразливість підприємства [1]. Особливо актуальним це стає в умовах масового переходу на віддалену роботу, що додатково ускладнює контроль за безпекою. Таким чином, сучасні виклики інформаційної безпеки підприємств є комплексними та багатогранними. Вони вимагають інтегрованого підходу до управління, який поєднує технологічні рішення, розвиток корпоративної культури та підвищення обізнаності персоналу. Лише за умов постійного вдосконалення систем захисту, адаптації до нових загроз і впровадження інноваційних підходів підприємства зможуть забезпечити стійкість своїх інформаційних систем у динамічному середовищі [5].

Людський фактор є однією з найважливіших складових інформаційної безпеки, яка водночас може бути і її найслабшою ланкою. Незважаючи на технологічний прогрес і впровадження сучасних систем захисту, роль співробітників у забезпеченні безпеки залишається критичною. Людський фактор охоплює як ненавмисні помилки, так і навмисні дії, які можуть спричинити витік або втрату інформації [3]. Найбільш поширеними прикладами ненавмисних дій є недотримання правил кібергігієни, таких як слабкі або однакові паролі, нехтування оновленнями програмного забезпечення, відкриття підозрілих електронних листів та посилань. З іншого боку, навмисні дії співробітників, зокрема передача конфіденційної інформації стороннім особам або її використання з метою власної вигоди, можуть мати катастрофічні наслідки для компанії [2].

Важливим аспектом людського фактора є також обізнаність працівників щодо актуальних кіберзагроз. Дослідження свідчать, що велика частина інцидентів у сфері інформаційної безпеки виникає через брак навчання персоналу. Умови, за яких співробітники не розуміють, як діяти у разі виявлення загроз або як мінімізувати ризики, створюють додаткову вразливість для підприємства [7]. Традиційні підходи до захисту інформації базуються переважно на технічних засобах, таких як антивірусні програми, фаєрволи, шифрування та регулярне резервування даних. Хоча ці інструменти залишаються важливими компонентами безпеки, вони мають низку недоліків, які стають критичними в умовах швидкого розвитку технологій і зростання кіберзагроз [6].

По-перше, традиційні системи захисту часто є реактивними, тобто реагують на загрози після того, як вони вже реалізовані. Такий підхід ускладнює превентивний захист, особливо у випадках складних і цілеспрямованих атак. По-друге, залежність від стандартних інструментів безпеки створює ризик, що вони не зможуть виявити нові види загроз, зокрема атаки, засновані на соціальній інженерії або експлуатації вразливостей у програмному забезпеченні. Третім недоліком є недостатня інтеграція традиційних підходів із організаційними аспектами. Відсутність ефективної політики управління інформаційною безпекою, відсутність навчання персоналу або нехтування культурою безпеки можуть значно знизити ефективність навіть найдосконаліших технологій. Нарешті, ще однією слабкістю є висока залежність від технічних засобів і недостатнє врахування людського фактора. Навіть найкращі технології не зможуть забезпечити захист, якщо співробітники не будуть дотримуватися встановлених правил або не усвідомлюватимуть свою роль у забезпеченні безпеки [7]. Таким чином, успішне забезпечення інформаційної безпеки вимагає від підприємств не лише використання новітніх технологій, але й приділення належної уваги людському фактору та впровадження сучасних, комплексних підходів, які враховують взаємозв'язок між технічними, організаційними та поведінковими аспектами [8].

Інтелектуальний капітал є невід’ємною складовою стратегії інформаційної безпеки сучасних підприємств. Його інтеграція в системи захисту інформації дозволяє поєднати технологічні, організаційні та людські ресурси для створення комплексного підходу до забезпечення безпеки даних. У сучасних умовах цифровізації взаємозв’язок між компонентами інтелектуального капіталу та елементами інформаційної безпеки стає дедалі важливішим, оскільки знання, компетенції, досвід та організаційні інновації формують основу для ефективного управління ризиками [3]. Людський капітал, що включає знання та компетенції співробітників, є ключовим у забезпеченні безпеки інформації. Працівники, які володіють актуальними знаннями про кіберзагрози та технологічні засоби захисту, можуть виявляти потенційні ризики та діяти превентивно. Наприклад, знання про соціальну інженерію або специфіку атак типу фішинг дозволяє мінімізувати ризики, пов’язані з людським фактором. У цьому контексті важливим є постійне навчання та підвищення кваліфікації персоналу, що формує їх здатність адаптуватися до нових викликів інформаційної безпеки [1]. Організаційний капітал також відіграє значну роль у формуванні надійної системи захисту. Політики та процедури, засновані на інноваційних підходах до управління безпекою, дозволяють забезпечити ефективну інтеграцію технологій у корпоративні процеси [5]. Наприклад, створення автоматизованих систем моніторингу загроз, використання програмного забезпечення для аналізу аномалій та впровадження шифрування даних є важливими елементами стратегії безпеки. Крім того, корпоративна культура, яка стимулює відповідальне ставлення до безпеки, сприяє підвищенню загальної стійкості підприємства до загроз.

Сучасні технології, такі як штучний інтелект (AI), аналітика великих даних (Big Data) та машинне навчання, відіграють вирішальну роль у підвищенні ефективності систем захисту інформації. Інструменти на основі AI можуть прогнозувати можливі загрози, аналізувати поведінкові моделі співробітників для виявлення відхилень і автоматизувати процеси управління ризиками. Наприклад, використання машинного навчання дозволяє виявляти невідомі раніше атаки, які не можуть бути ідентифіковані традиційними системами захисту. Аналітичні інструменти, у свою чергу, надають можливість обробляти великі обсяги даних, що допомагає формувати більш точні стратегії управління безпекою [4]. Інтеграція інтелектуального капіталу в інформаційну безпеку також передбачає використання клієнтського капіталу, який відображає довіру клієнтів та їхні очікування щодо захисту конфіденційної інформації. Сучасні компанії розуміють, що їхня репутація залежить від

здатності забезпечити надійний захист даних клієнтів. Це спонукає до впровадження не лише технічних рішень, але й створення відкритих комунікаційних політик щодо обробки та збереження даних [5].

Отже, інтеграція інтелектуального капіталу в стратегію інформаційної безпеки дозволяє формувати адаптивні, інноваційні системи захисту, які враховують як технологічні аспекти, так і роль людського фактора. Використання сучасних технологій у поєднанні з управлінням знаннями, досвідом і корпоративною культурою стає основою для забезпечення стійкості підприємств у динамічному середовищі ризиків [6]. Практичні рекомендації для підприємств, які прагнуть забезпечити належний рівень інформаційної безпеки через управління інтелектуальним капіталом, повинні враховувати два ключових аспекти: створення ефективної системи навчання персоналу та формування корпоративної політики, орієнтованої на мінімізацію ризиків [8].

Одним із першочергових завдань є створення системи навчання та підвищення кваліфікації персоналу у сфері інформаційної безпеки. Співробітники часто є слабкою ланкою у системі захисту, тому регулярні тренінги та навчання з основ кібербезпеки стають невід'ємною частиною стратегії підприємства. Наприклад, навчальні програми повинні охоплювати теми розпізнавання фішингових атак, безпечного використання корпоративних ресурсів, управління паролями, правил поведінки у разі виявлення загроз тощо. Важливим кроком є також симуляція реальних інцидентів, що дозволяє оцінити готовність персоналу реагувати на загрози. Крім того, необхідно впроваджувати індивідуальний підхід до навчання залежно від рівня доступу працівників до конфіденційної інформації [2]. Додатково варто використовувати сучасні платформи для онлайн-навчання, які забезпечують доступ до інтерактивних матеріалів, тестування та сертифікації. Це не лише підвищує кваліфікацію персоналу, але й сприяє формуванню культури безпеки в організації [4]. Іншим важливим аспектом є формування корпоративної політики управління інтелектуальним капіталом з урахуванням ризиків інформаційної безпеки. Така політика має включати комплексний підхід до управління знаннями, досвідом і технологіями в контексті захисту інформації. Перш за все, необхідно розробити чіткі регламенти щодо використання інформаційних систем, доступу до конфіденційних даних і зберігання інформації. Ці регламенти повинні бути прозорими та доступними для всіх співробітників [1]. Крім того, політика має враховувати ризики, пов'язані з людським фактором. Наприклад, обмеження доступу до критичних ресурсів для непідготовлених працівників, регулярний перегляд прав доступу та використання багатофакторної аутентифікації можуть значно зменшити вразливості. Окрему увагу слід приділяти процесам адаптації нових співробітників, які повинні проходити базове навчання з інформаційної безпеки та ознайомлюватися з політиками компанії з першого дня роботи.

Висновки. Інтеграція інтелектуального капіталу в стратегію інформаційної безпеки дозволяє підприємствам забезпечити стійкість до сучасних кіберзагроз. Людський капітал, який включає знання, досвід та компетенції працівників, є основою для формування ефективних систем захисту. Організаційний капітал, зокрема інноваційні технології, політики безпеки та корпоративна культура, забезпечує підтримку технічних та управлінських процесів. Використання сучасних технологій, таких як штучний інтелект та Big Data, сприяє прогнозуванню та запобіганню потенційним загрозам. Практичні рекомендації, наведені у статті, дозволяють підприємствам побудувати комплексну стратегію інформаційної безпеки, що враховує сучасні виклики цифрової економіки.

ЛІТЕРАТУРА

1. Jones M., Davis R. (2022). Corporate Culture and Information Security. Business Perspectives.

2. Khaminich S., Heti K. The knowledge economy as a factor for enterprise development in management system. PHILOSOPHY, ECONOMICS AND LAW REVIEW. 2023. Vol. 1. No. 1. P. 103–115.
3. Khaminich S., Sokol P., Hordiichuk S. Gender issues in the context of economic relation. Держава та регіони. Серія : Економіка та підприємництво. 2023. Вип. № 1 (127). С. 107–112.
4. Liu H., Zhao X. (2020). Artificial Intelligence in Threat Detection. Cybersecurity Advances.
5. Smith J., Brown L. (2021). Human Factor in Cybersecurity. Journal of Information Security.
6. Кошовий, Б. П. (2024). Економіко-політичний аналіз загроз інтелектуальній безпеці України в умовах воєнного стану. Scientific notes of Lviv University of Business and Law, (41), 213-224. URL : https://nzlubp.org.ua/index.php/journal/article/view/1198
7. Попова, О. Формування системи економічної безпеки підприємства та стратегії її становлення і розвитку. Розділ 1. Механізм функціонування підприємства в Україні та його інтеграція до світоіого економічного простору, 318. URL : http://212.1.86.13/jspui/bitstream/123456789/5672/1/kolektyvna_monographiya_2021__%D0%94%D0%9D%D0%A3.pdf#page=318
8. Хамініч С. Ю. Основні тренди освіти в системі економіки знань. Міжнародний науковий журнал «Інтернаука». Серія : «Економічні науки». 2023. № 5. URL : https://doi.org/10.25313/2520-2294-2023-5-8886.

REFERENCES

1. Jones M., Davis R. (2022). Corporate Culture and Information Security. Business Perspectives.
2. Khaminich S., Heti K. The knowledge economy as a factor for enterprise development in management system. PHILOSOPHY, ECONOMICS AND LAW REVIEW. 2023. Vol. 1. No. 1. R. 103–115.
3. Khaminich S., Sokol P., Hordiichuk S. Gender issues in the context of economic relation. Derzhava ta rehiony. Seriia : Ekonomika ta pidpryiemnytstvo. 2023. Vyp. № 1 (127). S. 107–112.
4. Liu H., Zhao X. (2020). Artificial Intelligence in Threat Detection. Cybersecurity Advances.
5. Smith J., Brown L. (2021). Human Factor in Cybersecurity. Journal of Information Security.
6. Koshovyi, B. P. (2024). Ekonomiko-politychnyi analiz zahroz intelektualnii bezpetsi Ukrainy v umovakh voiennoho stanu. Scientific notes of Lviv University of Business and Law, (41), 213-224. URL : https://nzlubp.org.ua/index.php/journal/article/view/1198
7. Popova, O. Formuvannia systemy ekonomichnoi bezpeky pidpryiemstva ta stratehii yii stanovlennia i rozvytku. Rozdil 1. Mekhanizm funktsionuvannia pidpryiemstva v Ukraini ta yoho intehratsiia do svitoioho ekonomichnoho prostoru, 318. URL : http://212.1.86.13/jspui/bitstream/123456789/5672/1/kolektyvna_monographiya_2021__%D0%94%D0%9D%D0%A3.pdf#page=318
8. Khaminich S. Yu. Osnovni trendy osvity v systemi ekonomiky znan. Mizhnarodnyi naukovyi zhurnal «Internauka». Seriia : «Ekonomichni nauky». 2023. № 5. URL : https://doi.org/10.25313/2520-2294-2023-5-8886.

Goch Pavlo Vitaliyovych
(Postgraduate student of PVNZ "European University")

Chaplyk Taras Volodymyrovych
(Postgraduate student of PVNZ "European University")

TITLE OF THE ARTICLE

Abstract. *The article examines the integration of intellectual capital into the strategy for ensuring information security of enterprises. The interrelationships between human, organizational and client capital and the components of information security are highlighted. Innovative approaches to information protection based on the knowledge and competencies of personnel are considered, as well as modern technologies that support intellectual capital management. Practical recommendations for enterprises are provided on improving the information security system in the context of digitalization and the growth of cyber threats.*

Keywords: *intellectual capital, information security, cyber threats, human capital, corporate culture, innovative approaches, digitalization.*