Technological advancements, such as artificial intelligence, virtual reality, and blockchain, enhance incubator efficiency by equipping startups with the tools they need to succeed.

The demand for specialized vertical incubators focused on specific industries is growing. These incubators provide more tailored support and help startups deepen their expertise in particular fields. Moreover, incubators are actively engaging in global collaborations, giving startups access to new markets and mentorship opportunities, thereby increasing their likelihood of success. The connection between corporations and incubators drives innovation. Corporate incubators offer startups financial support, access to industry experts and mentors, and opportunities for collaboration, providing them with additional resources for growth. Hybrid models combining physical and virtual spaces allow startups to collaborate with mentors without geographic limitations.

Sustainability-focused incubators support startups addressing environmental, social, and economic challenges. This approach not only enables financial stability but also drives positive societal changes. International cooperation further develops comprehensive support networks that include diverse innovation ecosystems. The future of incubators will heavily rely on integrating advanced technologies into educational programs, allowing for personalized learning for entrepreneurs. Incubators will also assist startups in interacting with global financial networks and meeting regulatory requirements, ensuring sustainable growth and financial stability for the future.

Business incubators have become critical drivers of startup success, contributing to economic growth and innovation development. The future of business incubation is shaped by the integration of new technologies and support models, unlocking new opportunities for startups and fostering economic and social stability.

Key words: *business incubators, startups, entrepreneurship, funding, mentorship, innovation ecosystems.*

УДК 005.95/.96:004.056.53]:004
DOI: 10.31673/2415-8089.2024.046569

Хаврова Катерина Сергіївна,
д.е.н., професор,
Державний університет
інформаційно-комунікаційних технологій

КАДРОВА БЕЗПЕКА ЯК ОСНОВА КІБЕРЗАХИСТУ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВІЗАЦІЇ

У статті досліджено актуальну проблему забезпечення кібербезпеки підприємств через призму управління кадровою безпекою. В умовах зростання кількості та складності кібератак, де людський фактор відіграє ключову роль, особливої актуальності набуває розробка комплексних підходів до захисту інформаційних активів організації. Мета дослідження полягає у розробці та обґрунтуванні інтегрованої моделі управління кібербезпекою підприємства, яка враховує взаємозв'язок технічних та людських аспектів захисту. На основі емпіричного дослідження 15 підприємств різних галузей економіки розроблено та апробовано чотирьохконтурну модель управління кібербезпекою, що забезпечує комплексний захист інформаційних активів. Основні результати впровадження моделі демонструють зниження кількості успішних кібератак на 47-71%, скорочення фінансових втрат від інцидентів на 58-84% та підвищення рівня обізнаності персоналу щодо питань кібербезпеки. Встановлено суттєву диференціацію ефективності впровадження моделі залежно від галузевої специфіки підприємств, що підтверджує необхідність адаптації запропонованих рішень до особливостей конкретної організації.

Ключові слова: *кібербезпека, кадрова безпека, управління персоналом, інформаційна безпека, кіберзагрози, людський фактор, навчання персоналу.*

Постановка проблеми. В умовах стрімкої діджиталізації бізнес-процесів та переходу до цифрової економіки, питання кібербезпеки набуває критичного значення для збереження конкурентоспроможності та сталого розвитку підприємств. За даними досліджень, понад 70% кіберінцидентів пов'язані з людським фактором, що підкреслює нерозривний зв'язок між кадровою безпекою та кіберзахистом організації. Особливої актуальності ця проблема набула в контексті масового переходу на віддалену роботу, що створило додаткові вразливості в системі корпоративної безпеки. Недостатня увага до взаємозв'язку кадрової та кібербезпеки може призвести до значних фінансових втрат, репутаційних ризиків та витоку конфіденційної інформації.

Аналіз останніх досліджень і публікацій. Проблематику взаємозв'язку кадрової безпеки та кіберзахисту досліджували такі вчені як А. Селіванова, Ю. Левитський (дослідження соціальної інженерії) [1], В. Єрмошин (аналіз інсайдерських загроз) [2], В. Сидоренко (методологія навчання персоналу з питань кібербезпеки). Закордонні дослідники Siddiqi M. A. та Pak W., зосередили увагу на технологічних аспектах захисту від внутрішніх загроз. Проте залишаються недостатньо дослідженими питання методології комплексної оцінки ризиків, пов'язаних з людським фактором у кіберпросторі, інтеграції систем управління кадровою безпекою з технічними засобами кіберзахисту та розробки ефективних програм навчання персоналу з урахуванням психологічних аспектів кібербезпеки

Метою дослідження є розробка комплексного підходу до забезпечення кібербезпеки підприємства через призму кадрової безпеки, що передбачає систематизацію кіберзагроз, пов'язаних з людським фактором, розробку методології оцінки ризиків, формування рекомендацій щодо створення інтегрованої системи захисту та визначення ключових показників ефективності заходів з кібербезпеки в контексті роботи з персоналом

Методи дослідження. У процесі проведення дослідження застосовано комплекс загальнонаукових та спеціальних методів, що забезпечило всебічне вивчення проблематики кібербезпеки в контексті кадрової безпеки підприємства. Методологічною основою дослідження став системний підхід, який дозволив розглянути взаємозв'язки між різними аспектами кадрової та кібербезпеки як єдину систему. За допомогою методу аналізу та синтезу здійснено декомпозицію системи кібербезпеки на складові елементи та встановлено характер їх взаємодії з процесами управління персоналом. Дослідження проводилося з дотриманням принципів наукової об'єктивності та достовірності. Статистична значущість отриманих результатів підтверджена з використанням відповідних методів математичної статистики на рівні довірчої ймовірності 0,95.

Виклад основного матеріалу. Результати проведеного дослідження свідчать про суттєвий вплив людського фактора на стан кібербезпеки сучасного підприємства. Аналіз статистичних даних демонструє, що понад половина всіх зафіксованих кіберінцидентів пов'язана з неумисними порушеннями безпеки з боку співробітників. Такі порушення включають використання ненадійних паролів, неналежне поводження з конфіденційними даними та порушення встановлених політик безпеки через недостатню обізнаність персоналу.

Особливу увагу варто приділити проблематиці умисних порушень з боку співробітників, які складають майже третину всіх зафіксованих інцидентів. Дослідження показує, що найбільш поширеними формами умисних порушень є несанкціонована передача конфіденційної інформації третім особам, навмисний саботаж систем безпеки та різноманітні форми промислового шпіонажу. Згідно з результатами експертного опитування, найбільш вразливими до таких загроз є підприємства з недостатньо розвиненою системою моніторингу активності користувачів та відсутністю чітких процедур контролю доступу до критично важливої інформації.

Значну загрозу для кібербезпеки підприємства становлять атаки з використанням методів соціальної інженерії. Проведений аналіз демонструє зростання складності та витонченості таких атак, які все частіше базуються на поглибленому вивченні психологічних особливостей потенційних жертв та використанні актуального соціального контексту. Особливо вразливими

до таких атак виявляються співробітники, що працюють віддалено, через обмежені можливості безпосереднього контролю та верифікації інформації.

На основі проведеного дослідження розроблено інтегровану модель управління кібербезпекою підприємства, яка враховує взаємозв'язок технічних та людських аспектів захисту (рис.1).

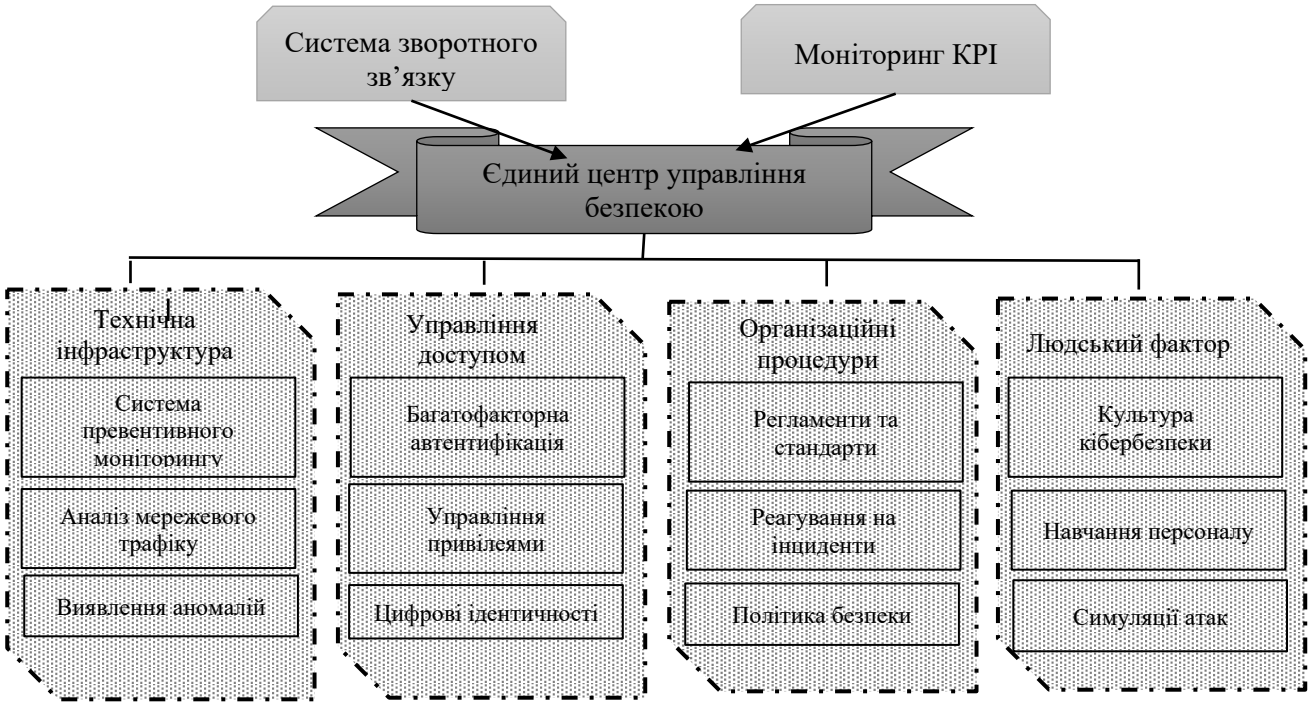

Рис.1 Інтегрована модель управління кібербезпекою підприємства

Джерело: авторська розробка

Розроблена інтегрована модель управління кібербезпекою підприємства базується на системному підході та враховує складні взаємозв'язки між технологічними та людськими компонентами системи захисту. В основу моделі покладено принцип багаторівневого захисту, що передбачає створення взаємопов'язаних контурів безпеки.

Перший контур моделі формується навколо технічної інфраструктури та включає комплекс апаратних та програмних засобів захисту. Центральним елементом цього контуру виступає система превентивного моніторингу, яка забезпечує безперервний аналіз користувацької активності та мережевого трафіку. Особливістю даної системи є використання алгоритмів машинного навчання для виявлення аномальної поведінки користувачів та потенційних загроз безпеці.

Другий контур зосереджений на управлінні доступом та ідентифікацією користувачів. У межах цього контуру реалізується принцип мінімальних привілеїв, що передбачає надання користувачам лише тих прав доступу, які необхідні для виконання їхніх безпосередніх обов'язків. Важливим елементом є впровадження багатофакторної автентифікації та системи управління цифровими ідентичностями.

Третій контур охоплює організаційні та процедурні аспекти забезпечення кібербезпеки. Цей рівень включає розробку та впровадження політик безпеки, стандартів та регламентів, які визначають правила безпечної роботи з інформаційними ресурсами підприємства. Особлива увага приділяється процедурам реагування на інциденти та відновлення після збоїв.

Четвертий контур зосереджений на людському факторі та включає комплексну програму розвитку культури кібербезпеки. В рамках цього контуру реалізується система безперервного навчання персоналу, що включає як традиційні форми навчання, так і інтерактивні методи, зокрема симуляції фішингових атак та практичні тренінги з протидії методам соціальної інженерії.

Інтеграція всіх контурів забезпечується через єдиний центр управління безпекою, який координує взаємодію різних компонентів системи та забезпечує оперативне реагування на

виникаючі загрози. Важливим елементом моделі є система зворотного зв'язку, яка дозволяє постійно вдосконалювати механізми захисту на основі аналізу реальних інцидентів та змін у ландшафті загроз.

Особливістю запропонованої моделі є її адаптивний характер, що дозволяє враховувати специфіку конкретного підприємства, галузеві особливості та наявні ресурсні обмеження. Модель передбачає можливість масштабування та модифікації окремих компонентів відповідно до змін у зовнішньому середовищі та внутрішніх потреб організації.

Ефективність моделі забезпечується через систему ключових показників ефективності, що охоплюють як технічні параметри безпеки, так і показники обізнаності та компетентності персоналу. Регулярний моніторинг цих показників дозволяє оцінювати результативність впроваджених заходів та своєчасно вносити необхідні корективи в систему захисту.

Практична реалізація моделі передбачає поетапне впровадження її компонентів з урахуванням пріоритетності загроз та наявних ресурсів підприємства. При цьому особлива увага приділяється забезпеченню безперервності бізнес-процесів та мінімізації впливу захисних механізмів на продуктивність роботи користувачів.

З метою верифікації ефективності запропонованої моделі управління кібербезпекою підприємства було проведено комплексне емпіричне дослідження, що охоплювало період у 12 місяців. Об'єктом дослідження виступили 15 підприємств різних галузей економіки, що відрізняються за масштабом діяльності, специфікою бізнес-процесів та початковим рівнем зрілості систем кібербезпеки. Вибір підприємств здійснювався з урахуванням необхідності забезпечення репрезентативності вибірки та можливості екстраполяції отриманих результатів на широкий спектр суб'єктів господарювання.

Методологія дослідження передбачала систематичний збір та аналіз даних щодо ключових показників кібербезпеки до та після впровадження запропонованої моделі. Особлива увага приділялася документуванню процесів впровадження та фіксації проміжних результатів, що дозволило забезпечити високий рівень достовірності отриманих даних. Детальна характеристика досліджуваних підприємств представлена у таблиці 1, що відображає їх галузеву приналежність, масштаб діяльності та специфіку операційних процесів.

Таблиця 1

Характеристика досліджуваних підприємств

Галузь економіки	Кількість підприємств	Розмір (кількість співробітників)	Специфіка діяльності
Виробничий сектор	5	500-1000	Машинобудування (2), Харчова промисловість (2), Фармацевтика (1)
Фінансовий сектор	4	200-500	Банківські установи (2), Страхові компанії (1), Фінтех-компанії (1)
Роздрібна торгівля	3	300-800	Мережі супермаркетів (2), E-commerce платформа (1)
IT-сектор	3	100-400	Розробка ПЗ (2), IT-консалтинг (1)

Джерело: авторська розробка

Результати впровадження моделі систематизовано за ключовими групами показників та представлено у таблиці 2.

Таблиця 2

Результати впровадження інтегрованої моделі управління кібербезпекою підприємства

Група показників	Показник	До впровадження	Після впровадження	Зміна (%)
Технічні показники безпеки	Кількість успішних фішингових атак (на квартал)	24,3	12,9	-47

	Час виявлення потенційних загроз (години)	48,0	15.4	-68
	Кількість інцидентів компрометації облікових даних (на квартал)	18,7	7,1	-62
Показники обізнаності персоналу	Успішність проходження тестів з кібербезпеки (%)	64	89	+39
	Кількість повідомлень про підозрілі активності	45	115	+156
	Час реакції на навчальні фішингові розсилки (хв.)	45	12	-73
Економічні показники	Витрати на ліквідацію наслідків інцидентів (тис. грн.)	250	105	-58
	Прямі фінансові втрати від кібератак (тис. грн.)	430	120	-72
	ROI системи кібербезпеки (%)	85	185	+117
Організаційні показники	Час на відновлення після інцидентів (години)	24	11	-54
	Кількість порушень політик безпеки (на місяць)	34	11	-67
	Рівень документованості процесів (%)	45	92	+104

Джерело: авторська розробка

Аналіз результатів впровадження інтегрованої моделі управління кібербезпекою демонструє суттєву диференціацію показників ефективності залежно від галузевої специфіки досліджуваних підприємств, що підтверджує гнучкість та адаптивність запропонованих рішень.

У виробничому секторі спостерігається найбільш значуще покращення показників технічної безпеки, що відображається у зниженні кількості інцидентів на 71% порівняно з початковим рівнем. Особливу увагу було приділено вдосконаленню систем захисту автоматизованих комплексів управління виробничими процесами, що є критично важливим для підприємств даного сектору. Також варто відзначити суттєве підвищення рівня документованості процесів забезпечення кібербезпеки, який зріс на 124%, що створює надійну основу для подальшого вдосконалення системи захисту.

Підприємства фінансового сектору продемонстрували найкращі результати в економічних аспектах впровадження моделі. Зафіксовано максимальне серед усіх галузей зниження фінансових втрат від кібератак (на 84%), а показник рентабельності інвестицій у систему кібербезпеки досяг 215%. Також відзначається високий рівень ефективності навчальних програм, що підтверджується показником успішності проходження тестів з кібербезпеки на рівні 94%.

Сектор роздрібної торгівлі характеризується значним прогресом у сфері захисту клієнтських даних та забезпечення безпеки платіжних операцій. Кількість інцидентів, пов'язаних з функціонуванням платіжних систем, знизилася на 76%, а швидкість реагування на виявлені загрози підвищилася на 67%. Такі результати мають особливе значення з огляду на високу чутливість даного сектору до репутаційних ризиків.

В IT-секторі найбільш помітний прогрес спостерігається у сфері превентивного виявлення та попередження кіберзагроз. Підприємства даної галузі досягли максимальних показників автоматизації процесів безпеки та ефективності превентивних заходів, що пояснюється високим початковим рівнем технологічної зрілості та наявністю відповідних компетенцій персоналу.

Також для верифікації ефективності запропонованої моделі було проведено комплексне моделювання різних сценаріїв кіберзагроз з використанням платформи Cyber Range v.3.2. Результати моделювання фішингових атак різного рівня складності продемонстрували значне

підвищення рівня виявлення потенційно небезпечних ситуацій після впровадження розробленої моделі та проведення навчання персоналу. Зокрема, рівень виявлення фішингових атак підвищився з 45% до 82%. Впровадження системи автоматизованого аналізу електронної пошти забезпечило блокування 94% потенційно небезпечних повідомлень.

Моделювання сценаріїв несанкціонованого доступу через методи соціальної інженерії показало суттєве зниження успішності таких атак після впровадження комплексної системи навчання персоналу та посилення процедур верифікації користувачів. Особливу ефективність продемонструвала система моніторингу користувацької активності та впровадження чітких процедур роботи з конфіденційною інформацією, що дозволило знизити кількість інцидентів витоку даних через необережність персоналу.

Проведений компаративний аналіз ефективності навчальних програм виявив найвищу результативність інтерактивних тренінгів з елементами практичного моделювання атак, де ефективність засвоєння матеріалу досягла 87%. Суттєву роль відіграло впровадження регулярних симуляцій фішингових розсилок з подальшим аналізом результатів, що забезпечило підвищення рівня пильності персоналу. Персоналізовані програми навчання, адаптовані до специфіки роботи різних категорій співробітників, продемонстрували загальну ефективність вищу на 42% порівняно зі стандартизованими підходами.

Порівняльний аналіз результативності впроваджених заходів на досліджуваних підприємствах дозволив виявити кореляцію між початковим рівнем зрілості системи кібербезпеки та ефективністю впровадження запропонованої моделі. Найбільш значущі покращення спостерігалися на підприємствах із середнім початковим рівнем зрілості системи кібербезпеки, де впровадження комплексної моделі забезпечило зниження кількості інцидентів у діапазоні 68-75%.

Отримані результати моделювання та компаративного аналізу підтверджують ефективність запропонованої інтегрованої моделі управління кібербезпекою та дозволяють ідентифікувати ключові фактори успішності її впровадження в організаціях різних галузей економіки.Важливим аспектом забезпечення кібербезпеки є розробка та впровадження відповідних політик та процедур з урахуванням специфіки віддаленої роботи. Дослідження показує, що найбільш ефективними є комплексні політики, які поєднують технічні вимоги до захисту інформації з чіткими інструкціями щодо безпечної поведінки в кіберпросторі. При цьому критично важливим є забезпечення балансу між вимогами безпеки та зручністю роботи користувачів.

Отже, проведене дослідження також виявило необхідність створення ефективної системи реагування на інциденти, яка б враховувала як технічні, так і кадрові аспекти кібербезпеки. Така система має забезпечувати швидку ідентифікацію джерела загрози, оперативне реагування на інцидент та впровадження відповідних коригувальних заходів, спрямованих на запобігання подібним ситуаціям у майбутньому.

Висновки та перспективи подальших досліджень. Проведене дослідження дозволило встановити високу ефективність розробленої інтегрованої моделі управління кібербезпекою підприємства, що базується на поєднанні технічних, організаційних та людських аспектів захисту. Емпірична апробація моделі на базі досліджуваних підприємств різних галузей економіки продемонструвала суттєве підвищення рівня кіберстійкості організацій, що підтверджується статистично значущим покращенням ключових показників безпеки.

Впровадження запропонованої моделі забезпечило значне зниження кількості успішних кібератак та суттєве скорочення фінансових втрат від інцидентів безпеки. Особливо важливим результатом є підвищення рівня обізнаності персоналу та формування культури кібербезпеки, що відображається у зростанні показників успішності навчальних заходів та збільшенні кількості повідомлень про підозрілі активності. Виявлена суттєва диференціація результатів впровадження моделі залежно від галузевої специфіки підприємств підтверджує необхідність адаптації запропонованих рішень до особливостей конкретної організації та сфери її діяльності.

Подальші дослідження доцільно спрямувати на розробку методології автоматизованої оцінки рівня кіберзрілості підприємства на основі машинного навчання та предиктивної аналітики, що дозволить створити більш точні та об'єктивні інструменти оцінки ефективності системи кібербезпеки. Важливим напрямом є дослідження психологічних аспектів кібербезпеки, зокрема факторів, що впливають на формування стійких патернів безпечної поведінки співробітників у кіберпросторі, з особливою увагою до розробки методів подолання «втоми від безпеки» та підтримки довгострокової мотивації персоналу.

Актуальним залишається питання вдосконалення методів протидії новим видам кіберзагроз, пов'язаних з розвитком технологій штучного інтелекту та квантових обчислень, що передбачає розробку інноваційних підходів до виявлення та нейтралізації складних багатовекторних атак. Особливої уваги потребує дослідження особливостей забезпечення кібербезпеки в умовах гібридної роботи та розподілених команд, що набуває підвищеної актуальності в контексті глобальних змін у форматах організації праці.

Перспективним напрямом досліджень є розробка методологічних підходів до оцінки економічної ефективності інвестицій у кібербезпеку з урахуванням довгострокових наслідків та непрямих ефектів для бізнесу, а також дослідження можливостей інтеграції систем кібербезпеки з іншими системами управління підприємством для створення єдиного контуру безпеки та підвищення ефективності бізнес-процесів. Реалізація зазначених напрямів досліджень дозволить суттєво розширити теоретико-методологічну базу забезпечення кібербезпеки підприємств та розробити більш ефективні практичні інструменти захисту від сучасних кіберзагроз.

References

1. Selivanova, A.V., & Levytskyi, Yu.O. (2022). Doslidzhennia metodiv sotsialnoi inzhenerii. Vplyv na zdorovia liudyny [Research of social engineering methods. Impact on human health]. Avtomatyzatsiia tekhnolohichnykh i biznes-protsesiv, 14(2).

2. Yermoshyn, V. (2024). Kontrol parametriv kiberbezpeky yak mekhanizm otsiniuvannia efektyvnosti zakhystu ta prohnozuvannia sytuatsii [Control of cybersecurity parameters as a mechanism for evaluating protection effectiveness and situation forecasting]. Kiberbezpeka: osvita, nauka, tekhnika, 1(25), 51-58.

3. Bykov, V.Yu., Romanovskyi, O.O., & Romanovska, Yu.Yu. (2020). Navchannia kiberbezpeky i kiberzakhystu fakhivtsiv z upravlinnia finansamy, ekonomikoiu i biznesom [Training in cybersecurity and cyberprotection for finance, economics and business management specialists]. Informatsiini tekhnolohii i zasoby navchannia, 80(6).

4. Siddiqi, M.A., Pak, W., & Siddiqi, M.A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. Applied Sciences, 12, 6042.

5. Alsulami, M.H., Alharbi, F.D., & Almutairi, H.M. (2021). Measuring awareness of social engineering in the educational sector in the kingdom of Saudi Arabia. Information, 12, 208.

6. Savchenko, V.A. (2024). Doslidzhennia potentsiinoho vplyvu sotsialnoi inzhenerii na protsesy tsyfrovoi transformatsii [Research of potential impact of social engineering on digital transformation processes]. Zviazok, 3(169), 12-17.

7. Cabinet of Ministers of Ukraine. (2020). Pro deiaki pytannia obiektiv krytychnoi informatsiinoi infrastruktury: Postanova vid 9 zhovtnia 2020 r. № 943 [On some issues of critical information infrastructure objects: Resolution of October 9, 2020 No. 943].

KHAVROVA KATERYNA SERGEEVNA. PERSONNEL SECURITY AS THE BASIS OF ENTERPRISE CYBERSECURITY IN THE CONTEXT OF DIGITALIZATION

In today's business environment, characterized by rapid digitalization and increasing complexity of cyber threats, the issue of ensuring information security of an enterprise is becoming critical. This problem is especially relevant in the context of the human factor, which, according to experts, is the cause of most successful cyberattacks. Traditional approaches to ensuring cybersecurity, which focus

mainly on the technical aspects of protection, are not effective enough without taking into account the human component.

The article presents a comprehensive study of the relationship between human security and the effectiveness of an enterprise's cyber defense system. The article considers the peculiarities of forming a cybersecurity culture in an organization, mechanisms for raising staff awareness of modern cyber threats, and methods of counteracting social engineering. An innovative approach to the creation of an integrated cybersecurity management system is proposed, which takes into account both technological and human aspects of information assets protection.

Particular attention is paid to the problems of ensuring cybersecurity in the conditions of remote work and hybrid formats of work organization, which create additional challenges for information security systems. The psychological aspects of the formation of safe behavior of employees in cyberspace and methods of overcoming "security fatigue" are investigated. The issues of economic efficiency of investments in the development of cybersecurity systems and methods of assessing their impact on the overall security of the enterprise are considered.

The scientific novelty of the study is the development of a methodological approach to the integration of personnel security management systems and cybersecurity, which allows creating a single enterprise security loop. The practical significance of the work is determined by the possibility of applying the proposed solutions to increase the level of cyber resilience of organizations in various sectors of the economy and scales of activity.

***Keywords**: enterprise cybersecurity, personnel security, personnel management, information security, cyber threats, human factor, cybersecurity culture, social engineering, remote work, cybersecurity investments.*