УДК 004.056:004.65:316.6
DOI: https://doi.org/10.32782/2413-9971/2025-58-12

Кальченко В.В.
старший викладач кафедри кібербезпеки
Сумського державного університету
ORCID: https://orcid.org/0000-0001-6492-3806
Балагуровська І.О.
аспірантка
Сумського державного університету;
Silesian University of Technology
ORCID: https://orcid.org/0000-0003-3642-9506
Маценко О.М.
кандидат економічних наук, доцент,
доцент кафедри економіки, підприємництва та бізнес-адміністрування
Сумського державного університету
ORCID: https://orcid.org/0000-0002-1806-2811
Кушнерьов О.С.
доктор філософії
Сумського державного університету
ORCID: https://orcid.org/0000-0001-8253-5698

Kalchenko Vadym
Senior Lecturer of the Department of Cybersecurity
Sumy State University
Balahurovska Inna
Postgraduate Student
Sumy State University;
Silesian University of Technology
Matsenko Oleksandr
PhD, Docent,
Associate Professor at the Department of Economics,
Entrepreneurship and Business Administration
Sumy State University
Kushnerov Oleksandr
Doctor of Philosophy
Sumy State University

СОЦІАЛЬНО-ПСИХОЛОГІЧНІ ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Анотація. У статті досліджено соціально-психологічні особливості впровадження систем управління інформаційною безпекою (СУІБ) на підприємствах. Автори обґрунтовують, що ефективність таких систем визначається не лише технічним оснащенням і нормативною базою, але передусім людським фактором, рівнем організаційної культури, довіри та психологічного клімату в колективі. У роботі узагальнено результати сучасних наукових досліджень, міжнародних стандартів серії ISO/IEC 27xxx та практичних кейсів з діяльності підприємств, які впроваджують політики інформаційної безпеки. Застосовано системний і міждисциплінарний підхід, що поєднує методи кібербезпеки, менеджменту та організаційної психології. Запропоновано класифікацію шести груп обмежень, які виникають у межах політик інформаційної безпеки та безпосередньо впливають на персонал. На основі аналізу емпіричних прикладів доведено, що надмірний контроль і регламентація призводять до підвищення рівня стресу, професійного вигорання, саботажу та руйнування довіри між співробітниками. Підкреслено, що суворі формалізовані політики без урахування соціально-психологічних сторін здатні нівелювати ефективність навіть найсучасніших технічних засобів захисту. Автори зазначають, що успішне функціонування СУІБ можливе лише за умови поєднання технічних, організаційних і поведінкових заходів, формування культури довіри, прозорості й усвідомленої відповідальності кожного працівника. У статті наголошено на потребі адаптивного підходу до впровадження інформаційної безпеки, який передбачає регулювання політик, навчання персоналу, розвиток психологічної стійкості працівників та інтеграцію принципів організаційної етики у щоденну практику менеджменту. Отримані

результати розширюють розуміння соціально-психологічних чинників у сфері кібербезпеки та можуть бути використані для вдосконалення корпоративних стратегій управління інформаційною безпекою і розвитку культури безпеки в організаціях.

Ключові слова: кібербезпека, інформаційна безпека, система управління інформаційною безпекою (СУІБ), психологічний клімат, менеджмент персоналу.

Вступ та постановка проблеми. В епоху цифрових технологій захист інформації в корпоративних мережах набуває нового значення та стратегічної важливості. На сучасному етапі розвитку економіки та науки актуальною є не лише проблема створення нових продуктів і технологій, але й забезпечення захисту результатів інтелектуальної діяльності (інформаційних ресурсів) для отримання конкурентних переваг.

У XXI столітті продуктом може бути не лише матеріальний об'єкт чи виробнича технологія, а й програмне забезпечення, бізнес-стратегії або організаційні інновації. З розвитком інформаційних технологій відомості про такі винаходи, товари та послуги зберігаються переважно на електронно-обчислювальних засобах, інтегрованих у глобальні інформаційно-комунікаційні мережі, що робить питання їх захисту особливо критичним. Забезпечення інформаційної безпеки спрямоване не лише на підтримку ефективного просування продуктів (послуг) на ринку, а й на збереження конкурентних переваг шляхом охорони критичної інформації, що може розкрити унікальні властивості пропонованих продуктів чи послуг.

Персонал компанії, який володіє цінною (конфіденційною) інформацією та працює з документами, що містять комерційну таємницю, є водночас носієм знань і потенційним джерелом витоків даних. Для мінімізації таких ризиків та формування стійкої системи захисту підприємство повинно впроваджувати цілісну політику управління інформаційною безпекою, що інтегрує організаційні, технічні та кадрові заходи.

Методи забезпечення інформаційної безпеки можна класифікувати за трьома основними складовими: організаційною, що передбачає роботу з персоналом; технічною, що охоплює використання спеціалізованих засобів захисту; та законодавчою, яка включає збір і застосування нормативно-правових актів для притягнення порушників до відповідальності (ISO/IEC 27xxx, 2018-2022). Для ефективного керування процесами інформаційної безпеки на підприємствах впроваджуються системи управління інформаційною безпекою (СУІБ), метою яких є мінімізація загроз та підтримання заданого рівня безпеки. Водночас невдале впровадження СУІБ може призводити до негативних наслідків, зокрема витоків інформації, морально-психологічного тиску на працівників та втрати керованості персоналом.

Аналіз останніх досліджень і публікацій. Сучасні дослідження у сфері інформаційної безпеки дедалі частіше зосереджуються на системах управління, що інтегрують технічні, організаційні та людські аспекти. Однією з найбільш поширених методологій є система управління інформаційною безпекою (СУІБ), що базується на стандартах ISO/IEC 27xxx (ISO/IEC 27xxx, 2018-2022), які формують рамки для побудови політик безпеки та процедур взаємодії з персоналом. Впровадження СУІБ не лише знижує ризики витоку даних, але й змінює структуру взаємовідносин у колективах та корпоративну культуру.

Значна увага приділяється людському фактору, оскільки саме помилки чи навмисні дії персоналу є причиною більшості інцидентів безпеки [2]. Зокрема, за даними дослідження Verizon, понад 70% витоків інформації пов'язані з діями співробітників, незалежно від їх намірів [3]. Подібні результати підтверджують і праці, що аналізують психологічні сторони сприйняття правил безпеки, а саме надмірний контроль та суворі політики можуть призводити до прихованого саботажу або формування апатії у працівників [4; 5].

Нагляд і контрольні механізми, що застосовуються в рамках СУІБ, мають потенціал створення так званого "ефекту спостереження", коли працівники почуваються постійно під контролем, що може негативно впливати на їх психоемоційний стан [6]. Дослідження в галузі організаційної психології показують, що постійний моніторинг може викликати підвищений рівень стресу, зниження ініціативності та навіть розвиток психосоматичних захворювань [7].

Питання етики та балансу між безпекою і комфортом персоналу піднімалися в ряді праць, які підкреслюють необхідність поєднання технічних рішень із заходами щодо підтримки довіри і формування культури безпеки [8]. Згідно з дослідженнями, найбільш успішні організації впроваджують СУІБ, орієнтуючись не лише на суворі обмеження, а й на навчання персоналу та розвиток усвідомленого ставлення до захисту інформації [9].

Крім того, питання впливу політик інформаційної безпеки на ефективність менеджменту все частіше аналізуються у контексті цифрової трансформації підприємств. Показано, що надмірна регульованість може призводити до втрати гнучкості, зростання конфліктності у колективах та падіння [10; 11]. Окремі дослідження навіть описують "організаційне вигорання", спричинене надлишковим контролем та відсутністю автономії працівників [12].

Отже, наукові джерела підтверджують необхідність балансу між безпекою інформаційних активів та збереженням здорового психологічного клімату в колективах. Для цього пропонується перехід від суто технократичного підходу до моделі, де безпека інтегрується в організаційну культуру та менеджмент персоналу [13; 14].

Методологія дослідження. Методологічну основу статті становить поєднання теоретичного

аналізу та якісних емпіричних спостережень. В роботі застосовано системний підхід, який дозволив комплексно розглянути взаємозв'язок між технічними, організаційними та соціально-психологічними чинниками впровадження систем управління інформаційною безпекою (СУІБ).

По-перше, здійснено аналіз наукових джерел і міжнародних стандартів (зокрема серії ISO/IEC 27xxx та ISO/IEC 27002:2022), що визначають рамки побудови політик інформаційної безпеки. Це дало можливість сформувати теоретичне підґрунтя для дослідження соціально-психологічних питань СУІБ.

По-друге, для ілюстрації практичного виміру використано узагальнені приклади з реальної діяльності підприємств, зібрані на основі авторських спостережень. Такі кейси подані в анонімізованій формі з огляду на конфіденційність інформації, проте вони відображають типові проблеми, що виникають у процесі впровадження та експлуатації СУІБ.

По-третє, для систематизації чинників впливу на персонал запропоновано класифікацію обмежень, що виникають у межах політик інформаційної безпеки. Такий підхід дозволив виявити причинно-наслідкові зв'язки між надмірним регламентуванням та психологічним станом працівників, а також визначити критичні зони ризику.

По-четверте, для інтерпретації впливу політик інформаційної безпеки на персонал застосовано методи організаційної та соціальної психології, що дозволило оцінити ризики, пов'язані з мотивацією, психологічним кліматом та рівнем довіри у колективі.

Таким чином, дослідження поєднало огляд літератури, аналіз нормативних документів, класифікацію обмежень, якісні емпіричні приклади та міждисциплінарний підхід, що забезпечило цілісне розкриття проблематики впливу СУІБ на ефективність діяльності підприємств.

Результати дослідження. Керівники підприємств переважно зосереджуються на економічних ризиках, пов'язаних із можливими фінансовими втратами, невиконанням договірних зобов'язань або зниженням прибутковості, водночас недооцінюючи ризики порушення інформаційної безпеки, зокрема загрози, що виникають через людський фактор і технічні недоліки [17; 18]. В умовах цифровізації навіть пересічний користувач корпоративної мережі може стати причиною витоку критично важливої інформації. З практичної точки зору, до такої інформації належать умови договорів і постачання продукції (послуг), вартість виконаних робіт, відомості про клієнтів і постачальників, а також технологічні особливості виробництва.

Згідно з концепцією інформаційної безпеки, інформація характеризується трьома базовими властивостями: конфіденційністю, цілісністю та доступністю. Під конфіденційністю розуміється можливість доступу до інформації лише уповноважених осіб, під цілісністю – забезпечення можливості внесення змін виключно тими користувачами, які мають відповідні права, а під доступністю – надання користувачам доступу до інформації відповідно до встановлених правил [19; 20]. Відповідно, основною метою керівництва є забезпечення зазначених характеристик критичних інформаційних активів.

Однак на практиці спостерігається тенденція фокусу менеджерів на технічних рішеннях, що сприймаються як гарантія повного захисту. При цьому залишається поза увагою той факт, що налаштування й експлуатація технічних засобів безпеки здійснюється самими працівниками, від рівня їхньої відповідальності та кваліфікації безпосередньо залежить ефективність функціонування системи [21].

В Україні для забезпечення інформаційної безпеки підприємства згідно законодавства можна застосовувати два підходи: побудову системи управління інформаційною безпекою (СУІБ) та з 2025 року (після відповідних змін в нормативних документах) – створення авторизованих систем безпеки.

Нині існує широкий спектр стандартів і методик, спрямованих на регламентацію дій персоналу задля зниження ризиків інформаційної безпеки. Водночас, як свідчать дослідження, їхнє жорстке або непродумане впровадження може мати зворотний ефект – погіршення психологічного клімату в колективі та зниження мотивації працівників [15]. Прикладом документа, що містить рекомендації щодо управління інформаційною безпекою, включаючи аспекти взаємодії з персоналом, є міжнародний стандарт ISO/IEC 27002 (2022), розроблений Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC).

На нашу думку, можна виокремити шість основних груп обмежень, що безпосередньо впливають на персонал (рис. 1). До таких обмежень належать:

– обмеження, пов'язані з роботою з комерційною таємницею;

– обмеження, що накладаються на працівників під час працевлаштування;

– обмеження, спрямовані на забезпечення фізичної безпеки підприємства;

– обмеження під час роботи з корпоративною комп'ютерною мережею;

– періодичні перевірки, які здійснюються співробітниками служби безпеки;

– проблеми міжособистої взаємодії, зумовлені психологічними особливостями та індивідуальними звичками працівників.

Відповідно до визначених на рисунку 1 груп обмежень, доцільно проаналізувати їх зміст та вплив на персонал більш детально.

1. Обмеження при роботі з комерційною таємницею. Під комерційною таємницею розуміють вид інтелектуальної власності, який включає формули, методи, процеси, конструкції, інструменти, шаблони або деякі компіляції інформації, що мають невід'ємну економічну цінність. Така таємниця не є загальновідомою або не може бути легко визначена іншими особами, а її володілець приймає розумні заходи з її збереження [22]. В свою чергу, в залежності від вартості комерційної таємниці, її важливості для володільців вживаються заходи

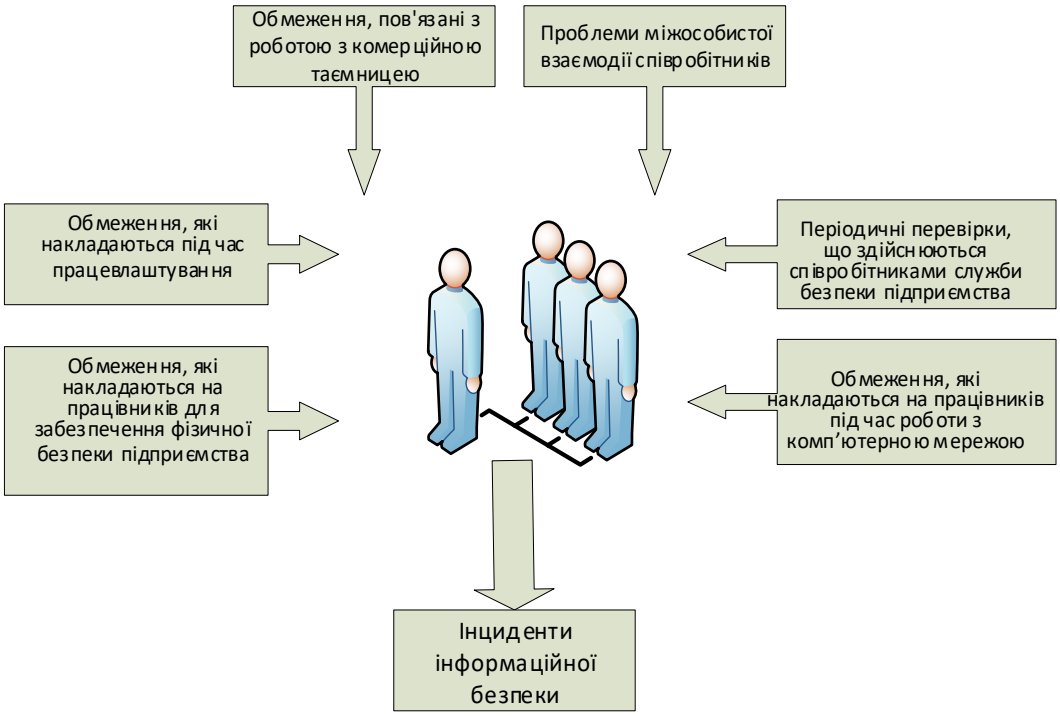

Рис. 1. Причинно-наслідкові зв'язки виникнення інцидентів інформаційної безпеки

Джерело: сформовано авторами

з її збереження. З точки зору обмежень які накладаються на персонал, такими заходами можуть бути:

– заборона для працівників допущених до комерційної таємниці обговорювати її у присутності осіб, які не допущені до неї;

– обговорювати з іншими особами (в тому числі з родичами) суть роботи, яку виконує працівник допущений до роботи з комерційною таємницею;

– передавати комерційну таємницю будь-яким способом до інших установ, підприємств, організацій або фізичним особам;

– обговорювати комерційну таємницю з використанням відкритих засобів зв'язку;

– фотографувати, сканувати, копіювати або іншим чином виготовляти копії носіїв комерційної таємниці;

– виконувати заходи із збереження носіїв комерційної таємниці відповідно до правил встановлених на підприємстві (наприклад працювати у виділених приміщеннях, зберігати відповідні документи в сейфі, тощо);

– обробляти документи, що містять комерційну таємницю на спеціально виділених засобах електронно-обчислювальної техніки;

– необхідність отримувати під підпис спеціально виділених електронних носіїв інформації та заборона вільного використання особистих зовнішніх електронних накопичувачів інформації;

– необхідність друкування документів з комерційною інформацією на попередньо врахованих аркушах паперу.

2. Обмеження, які накладаються під час працевлаштування. Міжнародний стандарт ISO/IEC 27002 (ISO/IEC 27002:2022, 2022) регламентує правила та методи роботи з персоналом для забезпечення конфіденційності, цілісності та доступності інформаційних активів на підприємстві. Цей стандарт виділяє три стадії взаємодії працівника та організації, що наймає його на роботу: працевлаштування, зайнятість та звільнення (рис. 2).

З точки зору безпеки, при прийомі на роботу необхідно максимально унеможливити потрапляння на роботу осіб, які можуть займатись крадіжками, махінаціями, торгівлею критичною для підприємства інформацією, тощо. Метою роботи з співробітниками на другому етапі є усвідомлення персоналом загроз і проблем пов'язаних з інформаційною безпекою, їх відповідальністю за порушення вимог інформаційної безпеки. На етапі звільнення важливо забезпечити впевненість в тому, що звільнені співробітники не будуть негативно впливати на безпеку інформаційних активів на підприємстві (ISO/IEC 27002:2022, 2022).

З практичної точки зору, стадії взаємодії з працівниками можуть передбачати наступні дії:

– перевірка автобіографічних даних працівника;

– перевірка наявності у працівника наявності судимостей;

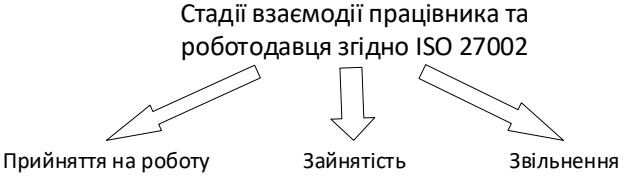

Рис. 2. Стадії взаємодії працівників та роботодавців

Джерело: сформовано авторами

– перевірка наявності оформлених кредитів;

– підписання договору про нерозголошення, який передбачає відповідальність працівника за розголошення тих чи інших відомостей про діяльність підприємства або відомостей, що становлять комерційну таємницю.

3. Обмеження, які накладаються на працівників для забезпечення фізичної безпеки підприємства. З точки зору забезпечення безпеки працівників, контролю за діями користувачів під час роботи з засобами електронно-обчислюваної техніки, унеможливлення проникнення на територію підприємства сторонніх осіб повинна бути впроваджені відповідні політики [23]. Вони передбачають, що територія підприємства (приміщення) повинні бути чітко поділені. Доступ працівників в критичні зони повинен бути чітко розмежований. Наприклад, працівники складу не мають право входу до приміщень бухгалтерії, відділу ІТ, тощо. При цьому фахівці відділу ІТ мають право входу до всіх приміщень, але при обов'язковій присутності не менше ніж одного працівника який постійно працює в такому приміщенні. Як правило, це вирішується за допомогою видачі кожному працівнику картки доступу [24]. З метою чіткої ідентифікації користувачів, контролю за їх діями під час роботи на комп'ютерах, працівникам також можуть видаватись smart-картки, або носії кваліфікованого електронного підпису. При цьому, якщо працівник втратить зазначені картки (носії), або залишить їх вдома, до нього можуть бути застосовані санкції як дисциплінарного так і матеріального характеру. Для контролю робочого часу, на підприємствах можуть використовуватись засоби контролю доступу, які фіксують час прибуття працівника на роботу, кількість виходів поза межі підприємства, тощо. Також для унеможливлення несанкціонованого доступу до приміщень у неробочий час, приміщення можуть опечатуватись, а ключі здаватись охоронцю з обов'язковим записом про це в відповідному журналі. З метою унеможливлення крадіжки носіїв комерційної таємниці, прибирання службових приміщень повинно здійснюватися виключно у присутності працівника, який працює у приміщенні. Для мінімізації можливості крадіжки матеріальних цінностей, на підприємстві може бути впроваджена політика щодо заборони внесення та виносу власних речей.

Окремо варто зазначити, що особливо деструктивний вплив на персонал мають грати на вікнах, захисні жалюзі, непрозоре скло в вікнах, приміщення без вікон або приміщення, яке розташоване в підвалі.

4. Обмеження, які накладаються на працівників під час роботи з комп'ютерною мережею. З метою забезпечення інформаційної діяльності підприємства, при роботі з комп'ютерною мережею на робочих комп'ютерах можуть встановлюватись програмні засоби які виконують наступні функції:

– контроль за діями на комп'ютері;

– заборона відвідування визначеного переліку сайтів;

– контроль за документами, які пересилають засобами електронної пошти, месенджерами, через веб-сайти, тощо;

– контроль за перепискою в месенджерах.

Крім того можуть впроваджуватись політики чистого робочого столу, чистого екрану монітора.

Подібні заходи дозволяють запобігти витокам конфіденційних даних та мінімізувати ризики внутрішніх порушень, пов'язаних із людським фактором [25]. Разом із тим, надмірний контроль може викликати зниження довіри між працівниками та роботодавцем і впливати на психологічний клімат у колективі [26]. Тому сучасні підходи рекомендують поєднувати технічні обмеження з навчанням персоналу та розвитком культури безпеки, а не покладатися виключно на засоби моніторингу. Важливо також забезпечити прозорість політик контролю, щоб працівники розуміли їхню мету та власну відповідальність у сфері інформаційної безпеки.

5. Періодичні перевірки, що здійснюються співробітниками служби безпеки підприємства. З метою забезпечення безпеки працівників та контролю за їхньою діяльністю в робочих приміщеннях можуть встановлюватися камери відеоспостереження та пристрої аудіозапису [27]. Для підвищення якості послуг часто здійснюється запис і подальший аналіз усіх телефонних переговорів, що ведуться за допомогою корпоративних засобів зв'язку. З метою запобігання витоку відомостей через відкриті джерела (OSINT) працівникам, як правило, забороняється публікувати в соціальних мережах інформацію про місце роботи та характер виконуваних завдань [28]. Для унеможливлення несанкціонованої роботи з конфіденційними даними на особистих пристроях може застосовуватися політика заборони внесення на територію підприємства власних смартфонів, ноутбуків, планшетів, фото- та відеотехніки.

Служба безпеки підприємства, як правило, складає плани-графіки раптових перевірок дотримання вимог політики безпеки, що, хоча й спрямовано на зниження ризиків інформаційних інцидентів, може негативно позначатися на психологічному стані працівників та викликати додатковий рівень стресу.

6. Проблеми міжособистої взаємодії співробітників пов'язані з особливостями психології, звичок працівників. Ефективна міжособиста взаємодія співробітників є важливою складовою успішного функціонування будь-якого підприємства, особливо в контексті забезпечення інформаційної безпеки. Однак особливості психології працівників, їхні звички, комунікативні стилі та міжособистісні конфлікти часто стають суттєвими бар'єрами для налагодження ефективної співпраці та впровадження систем управління інформаційної безпеки.

Психологічні чинники, такі як різниця у сприйнятті, стилях мислення, рівні емоційної інтелігентності, можуть призводити до непорозумінь і зниження рівня довіри між співробітниками, що у свою чергу негативно впливає на обмін інформацією та дотримання політик безпеки [29]. Звички, сформовані в процесі роботи, наприклад, нехтування

процедурними вимогами або використання неформальних каналів комунікації, створюють додаткові ризики витоку або несанкціонованого доступу до інформаційних активів [30].

Особливу увагу слід приділяти впливу стилю керівництва на психологічний стан працівників. Зокрема, дослідження Chan та McAllister (2014) показують, що «токсичне» або аб'юзивне керівництво формує у співробітників стан параної, що призводить до зниження рівня довіри, підвищення тривожності та формування ворожої атмосфери. Такий психологічний стан співробітників може негативно впливати на якість міжособистісної взаємодії і сприяти ігноруванню правил інформаційної безпеки. Відповідно, наявність аб'юзивного керівництва підвищує ризики внутрішніх загроз для інформаційних активів підприємства.

Крім того, міжособистісні конфлікти, зумовлені різними цінностями, мотиваціями або стилями поведінки, можуть сприяти формуванню токсичного клімату в колективі, що ускладнює впровадження та підтримання політик інформаційної безпеки [32]. Негативні емоції і стрес також впливають на уважність працівників до дотримання правил безпеки, збільшуючи ризики людської помилки.

Врахування психологічних особливостей та звичок працівників під час розробки заходів СМІБ дозволяє більш ефективно адаптувати методи мінімізації загроз, підвищити обізнаність співробітників та формувати культуру інформаційної безпеки на підприємстві [33].

В якості прикладів, можна привести такі випадки порушень вимог інформаційної безпеки, причиною яких стала саме наявність побудованої системи інформаційної безпеки та підвищених вимог до її забезпечення. Наведені приклади ґрунтуються на авторських спостереженнях та узагальненому досвіді підприємств, які з об'єктивних причин не можуть бути названі з огляду на конфіденційність інформації. Так, на великому підприємстві основною комерційною таємницею був перелік клієнтів та фінансові умови контрактів, однак у результаті перевірки виявилося, що доступ до відповідних документів мали всі користувачі мережі через неправильні налаштування прав доступу. В іншому випадку на підприємстві з електронним документообігом електронні довірчі підписи керівників зберігалися на незахищених носіях і були скопійовані системним адміністратором, що створювало серйозні ризики як репутаційних, так і матеріальних втрат. Наведені приклади є узагальненими кейсами з практики та демонструють, що навіть за наявності сучасних технічних засобів захисту відсутність належної культури інформаційної безпеки та навчання персоналу може призвести до критичних вразливостей.

Надлишковий контроль і суворе регламентування створюють у співробітників почуття «скляного ковпаку» або «цифрового паноптикума» [34], коли людина відчуває, що за нею постійно спостерігають. Дослідження показують, що вимушене дотримання жорстких правил безпеки збільшує стрес та негативно впливає на продуктивність персоналу [35]. Постійний психологічний тиск знижує мотивацію та задоволеність роботою, а у довгостроковій перспективі призводить до формування тривожних станів і психосоматичних симптомів (головні болі, порушення сну тощо). В умовах надмірного нагляду працівники втрачають відчуття автономії, а відсутність контролю над власною працею безпосередньо пов'язана з підвищенням стресу та професійним вигоранням [36].

Надмірні обмеження також породжують опірні й деструктивні реакції з боку персоналу. Коли співробітник відчуває себе не захищеним і несправедливо обмеженим, зростає рівень цинізму, розчарування та навіть агресії. Частина працівників реагує на жорсткий контроль саботажем і іншими формами девіантної поведінки. У таких умовах поширюється недовіра: люди починають сприймати колег і керівництво з підозрою, намагаються створювати «захисні бар'єри» (зайві перевірки, бюрократичні перепони) або навмисно ускладнювати робочі процеси. Гостро виявляються ситуації пасивно-агресивної поведінки: деякі працівники просто формально виконують мінімум обов'язків без ініціативи, в той час як інші відчувають фобії щодо будь-якого контакту з зовнішніми організаціями чи навіть колегами. Такі психологічні ефекти особливо небезпечні для колективу, адже відсутність довіри і підтримки в групі підвищує конфліктність і посилює ізольованість співробітників [37].

Від управлінського боку надмірна жорсткість політик безпеки часто дає протилежний очікуваному ефект. Хоча технічні заходи можуть бути сучасними, без належного психологічного супроводу вони призводять до падіння швидкості виконання завдань і якості роботи. Працівники, що постійно перебувають у стресі, допускають більше помилок і не наважуються проявляти ініціативу. Загальна атмосфера напруги викликає хронічне виснаження, низьку залученість у роботу і навіть фізичні захворювання, що в сукупності знижують ефективність менеджменту. Керівництво, яке фокусується на процедурному контролі, втрачає гнучкість у прийнятті рішень і змушене витрачати більше ресурсів на вирішення внутрішніх криз замість розвитку бізнесу.

Таким чином, надмірні обмеження в системі інформаційної безпеки призводять до зниження продуктивності та оперативності, адже працівники витрачають значну кількість часу на виконання формальних процедур і відчувають підвищену тривожність, що негативно позначається на швидкості виконання завдань та якості результатів. Така ситуація ускладнює атмосферу в колективі та провокує прояви саботажу, оскільки жорстке спостереження викликає опір. Співробітники можуть умисно ускладнювати робочі процеси, робити помилки або обмежуватись формальним виконанням обов'язків, що знижує рівень довіри й ефективність взаємодії в команді. Постійний стрес у такому середовищі сприяє розвитку психологічних розладів та емоційного вигорання, ускладнює концентрацію й викликає

фізичне виснаження. У результаті відбувається розпад колективної згуртованості, працівники дедалі більше орієнтуються на власні інтереси, уникають співпраці, що формує «атомізоване» середовище та підриває корпоративну культуру. Зрештою, жорсткі регламенти знижують гнучкість і мотивацію, підвищують плинність кадрів та ускладнюють контроль, через що керівники втрачають можливість ефективно мобілізовувати персонал, а правила сприймаються працівниками не як підтримка, а як загроза власним інтересам. Усі ці наслідки підтверджують, що надлишкове регулювання інформаційної безпеки без урахування психологічних та організаційних чинників здатне завдати більше шкоди, ніж користі, через зниження загальної ефективності діяльності підприємства.

Висновки. У статті досліджено вплив впровадження систем управління інформаційною безпекою (СУІБ) на діяльність підприємств із врахуванням не лише технічних, а й соціально-психологічних чинників. Проведений аналіз літератури та практичних кейсів показав, що ефективність заходів інформаційної безпеки значною мірою залежить від збалансованості між контролем і довірою, технічними обмеженнями та комфортом працівників, стандартизацією процесів і гнучкістю управління персоналом.

Встановлено, що надмірне застосування контрольних механізмів може призводити до демотивації, стресу, прихованого саботажу та погіршення психологічного клімату в колективі, тоді як ігнорування людського фактора здатне нівелювати навіть найефективніші технічні заходи захисту. Важливою умовою побудови дієвої СУІБ є інтеграція технічних, організаційних і поведінкових заходів в єдину політику безпеки, орієнтовану на культуру довіри та усвідомлену відповідальність персоналу.

Запропоновано класифікацію шести основних груп обмежень, що впливають на працівників у межах політик інформаційної безпеки, та проаналізовано їхній потенційний вплив на психологічний стан і продуктивність персоналу. Отримані результати підкреслюють необхідність адаптивного підходу до впровадження СУІБ, який включає врахування етичних норм взаємодії з працівниками, попередню оцінку технічних і соціальних ризиків, впровадження програм навчання та підвищення обізнаності персоналу, а також застосування інструментів організаційної психології для формування сприятливого мікроклімату.

Список використаних джерел:

1. International Organization for Standardization. (2018-2022). ISO/IEC 27xxx. Information security, cybersecurity and privacy protection – Standards family. ISO. Geneva. URL: https://www.iso.org/isoiec-27001-information-security.html
2. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.
3. Verizon (2021). Data Breach Investigations Report. Verizon Enterprise Solutions. URL: https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf
4. Pfleeger, S.L. & Caputo, D.D. (2012) Leveraging Behavioral Science to Mitigate Cyber Security Risk. *Computers & Security*, 31, 597–611.
5. Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. *International Journal of Information Security,* 24 (3). DOI: https://doi.org/10.1007/s10207-025-01032-0
6. Ball, K., Haggerty, K., & Lyon, D. (Ред.). (2012). Routledge Handbook of Surveillance Studies. Routledge. DOI: https://doi.org/10.4324/9780203814949
7. Ashkanasy, N. M., & Dorris, A. D. (2017). Emotions in the Workplace. *Annual Review of Organizational Psychology and Organizational Behavior*, 4 (1), 67–90. DOI: https://doi.org/10.1146/annurev-orgpsych-032516-113231
8. Ifinedo, P. (2014) Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition. *Information & Management*, 51, 69–79. DOI: https://doi.org/10.1016/j.im.2013.10.001
9. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66, 40–51. DOI: https://doi.org/10.1016/j.cose.2017.01.004
10. Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Applied Sciences*, 11 (8), 3383. DOI: https://doi.org/10.3390/app11083383
11. Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, 7 (3), e06522. DOI: https://doi.org/10.1016/j.heliyon.2021.e06522
12. Maslach, C., & Leiter, M. P. (2016). Understanding the Burnout Experience: Recent Research and Its Implications for Psychiatry. *World Psychiatry*, 15, 103–111. DOI: https://doi.org/10.1002/wps.20311
13. Alqaraleh, M. H., Almari, M. O. S., Ali, B. J. A., & Oudat, M. S. (2022). The mediating role of organizational culture on the relationship between information technology and internal audit effectiveness. *Corporate Governance and Organizational Behavior Review,* 6 (1), 8–18. DOI: https://doi.org/10.22495/cgobrv6i1p1
14. Willie, M. M. (2023). The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture. *SSRN Electronic Journal*. DOI: https://doi.org/10.2139/ssrn.4564291
15. Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging Behavioral Science to Mitigate Cyber Security Risk. *Computers & Security*, 31 (4), 597–611. DOI: https://doi.org/10.1016/j.cose.2011.12.010

16. International Organization for Standardization. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls. ISO. URL: https://www.iso.org/standard/75652.html
17. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems,* 18 (2), 106–125. DOI: https://doi.org/10.1057/ejis.2009.6
18. Hong, Y., & Furnell, S. (2019). Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization. *Journal of Computer Information Systems,* 1–10. DOI: https://doi.org/10.1080/08874417.2019.1683781
19. Kim, L. (2022). Cybersecurity: Ensuring Confidentiality, Integrity, and Availability of Information. In: Hübner, U.H., Mustata Wilson, G., Morawski, T.S., Ball, M.J. (eds) Nursing Informatics. Health Informatics. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-91237-6_26
20. Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security. *National Institute of Standards and Technology*. DOI: https://doi.org/10.6028/nist.sp.800-12r1
21. Mashiane, T., & Kritzinger, E. (2021). Identifying Behavioral Constructs in Relation to User Cybersecurity Behavior. *Eurasian Journal Of Social Sciences,* 9 (2), 98–122. DOI: https://doi.org/10.15604/ejss.2021.09.02.004
22. Lin, T. C. W. (2012). Executive trade secrets. *Notre Dame Law Review*, 87 (3), 911–970. SSRN 2047462. DOI: http://scholarship.law.ufl.edu/facultypub/122
23. Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards. Auerbach Publications. DOI: https://doi.org/10.1201/9780849390326
24. Bokhari, S. and Manzoor, S. (2022) Impact of Information Security Management System on Firm Financial Performance: Perspective of Corporate Reputation and Branding. *American Journal of Industrial and Business Management*, 12, 934–954. DOI: http://dx.doi.org/10.4236/ajibm.2022.125048
25. Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations. У Hawaii International Conference on System Sciences. Hawaii International Conference on System Sciences. DOI: https://doi.org/10.24251/hicss.2018.635
26. Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? ArXiv. URL: https://arxiv.org/abs/1901.02672
27. Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. *International Review of Law, Computers & Technology*, 28 (3), 277–298. DOI: https://doi.org/10.1080/13600869.2014.913874
28. Cross, M. (2014). Social media security : leveraging social networking while mitigating risk. Syngress.
29. Robbins, S.P. and Judge, T.A. (2016) Organizational Behavior. 17th Edition, Pearson Education Limited, Upper Saddle River.
30. Gerdenitsch, C., Wurhofer, D., & Tscheligi, M. (2023). Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior. Cyberpsychology: *Journal of Psychosocial Research on Cyberspace*, 17 (4), Article 7. DOI: https://doi.org/10.5817/CP2023-4-7
31. Chan, M. E., & McAllister, D. J. (2014). Abusive Supervision Through the Lens of Employee State Paranoia. *Academy of Management Review*, 39 (1), 44–66. DOI: https://doi.org/10.5465/amr.2011.0419
32. Riemenschneider, C. K., Burney, L. L., & Bina, S. (2023). The influence of organizational values on employee attitude and information security behavior: the mediating role of psychological capital. *Information & Computer Security*. DOI: https://doi.org/10.1108/ics-10-2022-0156
33. Whitman, M.E., Mattord, H.J. (2017). Principles of Information Security, 6th Edition. Cengage Learning.
34. Robbins, S.P. and Judge, T.A. (2016). Organizational Behavior. 17th Edition, Pearson Education Limited, Upper Saddle River.
35. Seung C. Lee (2024) Stress implications of compliance with information security policie. *Issues In Information Systems*. DOI: https://doi.org/10.48009/1_iis_2024_105
36. Maslach, C. (2017). Finding solutions to the problem of burnout. *Consulting Psychology Journal: Practice and Research*, 69 (2), 143–152. DOI: https://doi.org/10.1037/cpb0000090
37. Glavin, P., Bierman, A., & Schieman, S. (2024). Private Eyes, They See Your Every Move: Workplace Surveillance and Worker Well-Being. *Social Currents.* DOI: https://doi.org/10.1177_23294965241228874

SOCIO-PSYCHOLOGICAL FEATURES OF IMPLEMENTING INFORMATION SECURITY MANAGEMENT SYSTEMS

Summary. The article examines the socio-psychological features of implementing information security management systems (ISMS) in enterprises. The authors argue that the effectiveness of such systems is determined not only by technical equipment and the regulatory framework, but primarily by the human factor, including the level of organizational culture, trust, and psychological climate within the team. The paper summarizes the results of modern scientific research, international standards from the ISO/IEC 27xxx series, and practical cases from enterprises implementing information security policies. A systemic and interdisciplinary approach is applied, combining methods of cybersecurity, management, and organizational psychology. A classification of six groups of restrictions that arise within the framework of information security policies and directly affect personnel is proposed. Based on the analysis of empirical examples, it is proven that excessive control and regulation lead to an increase in stress levels, professional burnout, sabotage, and the erosion of trust between employees. It is emphasized that strict, formalized policies, without taking into account the socio-psychological aspects, can undermine the effectiveness of even the most modern technical means of protection. The authors note that the

successful functioning of the ISMS is possible only if technical, organizational, and behavioral measures are combined, a culture of trust is established, transparency is maintained, and a conscious responsibility is assumed by each employee. The article emphasizes the need for an adaptive approach to implementing information security, which involves regulating policies, training personnel, developing employee psychological resilience, and integrating organizational ethics principles into daily management practices. The results obtained expand the understanding of socio-psychological factors in the field of cybersecurity and can be used to improve corporate strategies for information security management and the development of a security culture in organizations.

Keywords: cybersecurity, information security, information security management system (ISMS), psychological climate, personnel management.

Стаття надійшла: 18.11.2025
Стаття прийнята: 10.12.2025
Стаття опублікована: 30.12.2025