КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.895
УДК 177 +17.03 + 378 + 004.03/.05

Козубцова Леся Михайлівна
кандидат технічних наук, доцент
завідувач кафедри математики та фізики
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0000-0002-7866-8575
l.kozubtsova@i.ua

Ліщина Валерій Олександрович
кандидат технічних наук, доцент,
завідувач кафедри комп'ютерних наук
Луцький національний технічний університет, Луцьк, Україна
ORCID: 0000-0002-2371-3850
lvaleriy@gmail.com

Козубцов Ігор Миколайович
доктор педагогічних наук, старший науковий співробітник,
професор кафедри комп'ютерних наук
Луцький національний технічний університет, Луцьк, Україна
ORCID: 0000-0002-7309-4365
kozubtsov@gmail.com

ВІД ОБІЗНАНОСТІ ДО УПРАВЛІННЯ: КОНЦЕПЦІЯ ЛЮДСЬКИХ РИЗИКІВ В СИСТЕМІ КІБЕРЗАХИСТУ

Анотація. Автори наукової статті звернули увагу, що незважаючи на війну в Україні суспільство адаптувалося до епохи інформаційних технологій, комп'ютеризація і автоматизації, цифровізація охопила всі аспекти життя людини. Концепція держава в смартфоні все більше реалізовується на різні державні послуги для населення. Послуги із соціальної сфери активно трансформується і застосовуються навіть у військовій сфері. Однак з ростом цифровізації виникає потреба розробляти контрзаходи з зміцнення інформаційної та кібербезпеки, і в першу чергу через людський фактор. Метою статті є вивчення психолого-педагогічної проблеми людського чинника забезпечення інформаційної безпеки та кібербезпеки. Результат дослідження. Проблема людського ризику у професійній діяльності не є новою. Людський фактор, закономірності та індивідуальні фактори, що впливають на професійну діяльність, її вплив на результат діяльності вивчалися теорією професійної психології. В епоху інформаційних технологій людський фактор є джерелом нових небачених раніше загроз. Як засвідчує сучасна практика, у гібридній війні супротивник до 90% інформації здобуває завдяки соціальної інженерії, отримує цінну інформацію через соціальні мережі (Facebook, Telegram-канал, Instagram, WhatsApp, Meta, YouTube), що була передана через необережні розмови. Ось чому досвідчені світові команди з кібербезпеки замислилися над рішенням задачі про зменшення людського ризику в інформаційній системі задля збереження захисту інформації та кібербезпеки. Так започаткувалася теорія управління людськими ризиками, поняття яке закріплене як окрема категорія, незалежне від навчання з підвищення обізнаності в галузі безпеки, управління людськими ресурсами обіцяє забезпечити більшу віддачу від інвестицій, ніж будь-яка інша стратегічна ініціатива в галузі безпеки. За результатами дослідження стає очевидним потреба впроваджувати «управління ризиками, пов'язаними з людським фактором». Управління ризиками для людини слід зосереджувати на результатах, а не лише на дотриманні вимог та кількісно визначати ризик, пов'язаний з людською поведінкою. Теоретичні та практичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого її вивчення в різних аспектах.

Ключові слова: захист інформації; кібербезпека; людський фактор; інформаційна система; інформаційні технології.

ВСТУП

В даний час, ми повсякденно увійшли в епоху інформаційних технологій (ІТ), комп'ютеризація і автоматизація повсюдно впроваджуються у всі аспекти життя людини. Зараз майже неможливо уявити життєдіяльність людини без ІТ. Все більше і більше цифровізуються різні державні послуги для населення. Важко переоцінити значимість ІТ у розвитку та позитивному існуванні людства. ІТ із соціальної сфери активно трансформується і застосовуються у військовій сфері держави. В цілому, як показують тенденції, роль ІТ буде тільки рости і між тим потрібні будуть контрзаходи зі зміцнення кібербезпеки.

Соціологічні дослідження встановили, що люди щодня проводять більше чотирьох годин зі своїми смартфонами [1], телевізійні інформаційні канали тануть в соціальних мережах (Facebook, Telegram, Instagram, WhatsApp, Meta, YouTube). Ця цифра варіюватися в різних країнах від можливостей і потреб самих людей. В Україні впроваджено державний мобільний застосунок Дія (скорочення від «Держава і я», англ. Diia), вебпортал і бренд цифрової держави в Україні, розроблений Міністерством цифрової трансформації України. Такий захід від держави спонукав громадян приділяти більше уваги своїм ґаджетам, навіть часом довіряють державі приватну інформацію, а іноді навіть конфіденційну – деякі користувачі для зручності прив’язують до смартфонів свої платіжні карти або вирішують прості робочі завдання – ставлячи електронний підпис через «ДІЮ». Однак, застосування ІТ нерозривно пов'язано із появою все нових видів загроз інформаційної безпеки (ІБ) та кібербезпеки (КБ). Не лише конфіденційна, а й будь-яка інформація, що потрапила в руки злочинців, становить під заразу життєдіяльність власника інформації.

Не виконуючи головне завдання ІБ – забезпечення конфіденційності, доступності та цілісності інформації, не можне гарантувати застосування ІТ в суворій відповідності з їх початковими цілями. У зв’язку із цим, потрібно докласти максимум зусиль для того, щоб забезпечити надійний рівень конфіденційності ІТ-систем. Сьогодні не існує універсальної методики забезпечення захисту, яка надавала б 100% гарантію безпеки [2]. Відповідно, інформаційна система захисту потребує постійного вдосконалення і покращення. Адже, хакери і злочинні елементи безперервно вдосконалюють власні методики злому і несанкціонованого проникнення. І цьому наочний приклад гібридної війни, поширення дезінформації та кібератак – все це становить серйозну загрозу для стабільності та суверенітету держави [3].

Аналіз останніх досліджень і публікацій. Проаналізуємо роботи, у яких приділено значної уваги до розв’язання проблеми обмеженої предметом дослідження.

У фундаментальній науковій праці доктора технічних наук, професора, академіка НАН України М. Згуровського, під інформаційною безпекою прийнято розуміти такий стан інформаційного середовища, при якому гарантується розвиток цього середовища і його використання в інтересах особи, суспільства і держави, а також захищеність від будь-яких загроз [4]. Відповідно основні заходи щодо захисту інформації (ЗІ) прийнято поділяти на організаційні та технічні. Варто зазначити, що крім «технічного» розуміння ІБ [4] існують альтернативні думки навіть ще у стані філософському осмислення ролі ІБ в житті сучасної людини [5], хоча відверто цей час давно вже минув, а сучасна реальність диктує потребу у підвищені вимоги до захисту інформації а від звичайної людини обізнаності – кіберігієни. До організаційних прийнято відносити регламентування з питань ІБ, а до технічних – застосування різних засобів захисту інформації, таких як засоби ЗІ від несанкціонованого доступу, засоби антивірусного захисту, міжмережеві екрани, системи

виявлення та запобігання вторгнень і т.д., а також об'єднання таких засобів в єдині комплексні системи ЗІ. Все це в сукупності створює «фортецю по захисту інформації», але, як і в давнину, слабким місцем завжди був і є людина. В сучасному світі користувач або посадова особа, що відповідає за захист інформації (далі – відповідальний за ЗІ), можуть знизити або зовсім звести нанівець ефективність всіх заходів, які передбачені для належного застосування щодо ЗІ.

Високу оцінку впливу людського фактора (ЛФ) на ІБ стали давати відносно недавно, і в даний час точне визначення терміну ЛФ так і не сформовано як одиницю дефініції. Людський фактор – поняття, що набуває останніми роками все більшого розголосу і значення у сфері кібербезпеки. Ускладнення виробничого обладнання, розвиток ІТ призводять до зростання ролі штучного інтелекту (ШІ) та до зниження ролі людини, вимог до професійної підготовки та надійності людини-оператора [6]. Отже, поняття ЛФ зводиться до можливості впливу людини на інформаційну систему, в тому числі на її захищеність. Зазвичай вплив ЛФ носить ненавмисний характер, що полягає в помилці дій людини, але в той же час має місце і варіант усвідомлених дій суб'єкта, коли адміністратори безпеки не можуть передбачити ті чи інші деструктивні дії користувачів.

Необхідно відзначити факт появи різних технічних засобів, спрямованих на мінімізацію ЛФ, таких як криптографічні перетворення інформації усередині інформаційної системи (ІС), системи запобігання від витоків інформації, системи контролю дій користувачів з підвищеними привілеями та інші. У різних джерелах кількість комп'ютерних інцидентів, пов'язаних з ЛФ, в тому числі і під впливом соціального інжинірингу, приймає значення близько 50 відсотків [4].

Через недостатнє врахування психологічних, психофізіологічних, антропометричних та інших властивостей людини-оператора в конструкції систем управління відбувається приблизно 30-40% усіх помилок внаслідок людського фактора в авіації, більше 60% транспортних пригод із важкими наслідками, більше 50% аварій в енергосистемах [6]. При цьому вітчизняні дослідники відзначають, що в Україні в два рази більше випадків витоку інформації, що захищається з вини саме непривілейованих внутрішніх користувачів [7].

Наявність людського фактора має першорядне значення в теорії інформаційної безпеки. Внаслідок дії людського фактора, так наприклад згідно Закону України «Про основні засади забезпечення кібербезпеки України» [8] є подією або ряд несприятливих подій ненавмисного характеру створює передумови до появи інцидент кібербезпеки таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів. Отже, можна вважати що в забезпечення надійної кібербезпеки ключова роль не належить лише машинам чи технологіям, це скоріше сумісна робота з участі людині (адміністратора та користувачів) [9]. Людський фактор, як такий залежить від багатьох, як внутрішніх так і зовнішніх, змінних а іноді може проявлятися у «ніби» нелогічних діях. Хоча при детальнішому аналізі прослідковується певна закономірність та послідовність подій.

В умовах російсько-української війни, справедливості раді, варто враховувати заявлені результати дослідження «Лабораторії Касперського», що ЛФ посідає почесне друге місце серед причин подій в області інформаційної безпеки РФ після шкідливого програмного забезпечення [10]. Цікавим є також досвід як з точки зору застосування

навмисних деструктивних впливів у відповідь зосередившись на тому, що як працівники роблять бізнес вразливим зсередини за рахунок ЛФ [11]. Отже урок на майбутнє з цього, що заходи від майбутніх кіберзагроз мають бути орієнтовані на працівників, такі як залучення та навчання співробітників, є одними з най дієвих тактик.

Збіжність думок спостерігається автора монографії до повномасштабного вторгнення [12]. Тож на майбутні успіхів в проведенні саме інформаційних та кібервиливів варто розраховувати через несвідомий або свідомий виток цінної інформації для супротивника. Свого часу британський математик та розробник системи, яка зламувала шифри Енігми А. Тюрінг висловив «Тисячі житті були втрачені в останній війні, тому що цінна інформація була передана ворогу через необережні розмови», який відображено на одному зі стендів музею Блетчлі Парку в Англії (рис. 1) [13]. Як засвідчує сучасна практика у гібридній війні супротивник до 90% інформації здобуває завдяки соціальної інженерії через ті ж самі соціальні мережі (Facebook, Telegram-канал, Instagram, WhatsApp, Meta, YouTube), доречним є приклад дослідників В. Бурячок, О. Корченко, Л. Бурячок опублікований 2012 р. у журналі «Захист інформації» [14].

Рис. 1. Вислів А.Тюрінгу зі стенду музею Блетчлі Парку в Англії

У той же час ЛФ як явище, пов'язане зі специфікою свідомості, мислення та особливостей людини, може виникати з різних причин. Багато вчених займаються дослідженнями філософських, соціальних, психологічних та інших причин, що спряють ЛФ, в тому числі і з боку етики. Наприклад, українські науковці Є. Живило, Л. Козубцова та В. Куцаєв наголошують про моральні та етичні принципи забезпечення безпеки інформації як: уникнення втрат активів, нерозповсюдження небезпечного, добросовісне використання і збереження таємниці [15; 16]. Вони, зокрема, прийшли до висновків, що морально-етичні якості посадових осіб безпосередньо впливають на інформаційну та кібербезпеку. Згодом дослідники Е. Анашкін, С. Забара, В. Куцаєв, К. Нестеров, Т. Терещенко, П. Хусаїнов та О. Черноног рекомендують проводити навчання етичних питань та аспектів інформаційної безпеки (кібергігієни) зі школи [17].

Група дослідників А. Баришева, Л. Веселова, Ю. Гладка, О. Довгань, А. Каленський, Ю. Матюхіна, О. Скибун, А. Тарасюк, Н. Троянска, Е. Фаулер, П. Френкен, Н. Шредер, Ю. Щавінський висувають гіпотезу про потребу окремо виділяють нові якості, що впливають на захищеність інформаційних технологій, такі як інформаційна моральність і етика [18], мотивація [15, 16] потрібно долучити фізичну втому адміністратор від безпеки [19], що може призвести до ненавмисного пошкодження

інформаційної безпеки. Автори дослідження [20] погоджуються, що співробітники організації часто є слабкою ланкою в захисті її інформаційних активів. Інформаційній безпеці не приділялося достатньо уваги в літературі з точки зору впливу людського фактора; дослідники закликають до подальшого вивчення цієї галузі. Людський фактор відіграє значну роль у комп'ютерній безпеці. Тому автори зосереджують увагу на з'ясуванні взаємозв'язку людського фактора з інформаційною безпекою, представляючи людські слабкості, які можуть призвести до ненавмисної шкоди організації, та обговорюючи, як обізнаність з інформаційної безпеки може бути основним інструментом у подоланні цих слабких місць.

Виділення невирішених раніше частин загальної проблеми, якій присвячується стаття. Слід зазначити, що в оглянутих роботах [4-20] підкреслюють важливість впливу ЛФ, а також таких аспектів, як інформаційні моральність і етика на безпеку інформації та інформаційних систем. Однак, чіткий взаємозв'язок між ними, а також повний перелік конкретних причин їх негативного впливу на захищеність інформації та шляхи рішення на даний момент не сформульовані. Нам видається важливим поглянути глибше на причини формування згубних проявів ЛФ, таких як халатності, недисциплінованість і низька виконавча дисципліна в частині виконання вимог з інформаційної безпеки та все частіше стає перевтома людини.

Зв'язок дослідження з важливими науковими завданнями. Отже, враховуючи потенційну проблему людського чинника забезпечення інформаційної безпеки, а також підставою до вивчення даної проблеми є рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» [21] та вимоги закону України «Про основні засади забезпечення кібербезпеки України» [8], а отже на вирішення цього завдання і буде зорієнтоване наше дослідження.

Мета статті. Метою статті є вивчення психолого-педагогічної проблеми людського фактора у забезпеченні інформаційної та кібербезпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В дійсній роботі, як і у соціально-гуманітарних науках, будемо розглядати ЛФ як причину помилкових дій, а також як психологічні та інші характеристики людини, його можливості й обмеження, які визначаються в конкретних умовах його діяльності.

У даній статті під людським фактором будемо рекомендувати розуміти всі можливі дії людини як умисні, так і неусвідомлені, які призводять або можуть призвести до негативних наслідків з точки зору функціонування ІС. Для захисту від ЛФ застосовуються організаційні і технічні заходи, однак, так як ЛФ носить стихійно-непередбачуваний характер, то і передбачити всі можливі варіанти впливу, а отже, передбачити і вибудувати гарантований захист надзвичайно важко.

Як правило, до причин суб'єктивного характеру, що породжує ЛФ у сфері ЗІ, відносять: особистісні особливості людини (психоемоційний стан, рівень дисциплінованості та відповідальності, кваліфікацію, вміння працювати в різних стресових ситуаціях з великим об'ємом інформації в умовах обмеженого часу, взаємини в колективі, систему цінностей людини тощо). Також необхідно вказати і вплив умов зовнішнього середовища (система може бути побудована так, що провокує прояви ЛФ, наприклад, надмірно велике навантаження, не відповідна можливостям людини, постійне відволікання від своєї основної діяльності, відсутність заохочень або покарання за розумну ініціативу і т. д.).

Причинами появи таких проблем можуть виступати різні психічні особливості, інтелектуальні обмеження можливостей, а також необізнаність людини. Наприклад, можливі такі ситуації: користувач відкриває шкідливе вкладення в провокаційному електронному листі, так як не розуміє можливі наслідки; користувач (відповідальний за ЗІ) справляє руйнівні дії на інформаційні ресурси ІС у зв'язку з психоемоційним стресом або усвідомлено переслідуючи корисливі цілі за винагороду, також це може виникати із-за низької адаптації в соціумі даної ІС; вчинення помилки при експлуатації ІС (засобів ЗІ) з-за великого обсягу паралельних завдань, а також різних відволікаючих факторів зовнішнього середовищ, наприклад надмірне захоплення в онлайн гру, перебуваючи на об’єктах критичної інформаційної інфраструктури [22].

Пропонуємо розглянути причини появи вищевказаних проблем з іншого боку.

Досить часто користувачі ІС задаються низкою питань. Навіщо настільки складні, що заважають працювати, засоби (методи) захисту інформації? Чому такі жорсткі (на їх погляд) вимоги до ЗІ? Всі вимоги до ЗІ створені, тільки щоб заважати користувачам? Який сенс від цих вимог, якщо противник, і так вже знає те, що хоче знати?

Зауважимо, що, не знаючи й не розуміючи складну структуру і процеси ІС, встежити за взаємозалежністю засобів ЗІ і елементів ІС дуже важко. Користувачі часом не замислюються про те, щоб їх робота в ІС була захищена, їм головне виконати свої завдання в строк. А так як супротивник у сфері ІТ майже завжди невидимий, то і ступінь ефективності і корисності засобів ЗІ користувач не відчуває.

Мало того, що такі питання задають собі користувачі, але все частіше зустрічається, коли подібні питання задають собі відповідальні за ЗІ. Навіщо я цим займаюся, якщо потенційний противник все одно все зламає і дізнається? Який сенс від моїх дій, адже у широкому розумінні на загальну інформаційну безпеку організації вони не вплинуть і т. д.

У цьому випадку відповідальні за ЗІ, від яких залежить точне і повне налаштування засобів ЗІ, не розуміють сенсу виконання в повній мірі всіх вимог, що в свою чергу спричиняє не повне виконання того, що пропонується контрольними прикладами налаштування.

Відбувається нерозуміння важливості своєї ролі у системі захисту інформації організації. Крім того, позиція «здатися без бою» призводить до неусвідомленої недбалості в частині адміністрування безпеки інформації, що в свою чергу веде до підвищення ймовірності негативного вплив людського фактору.

Спробуємо виділити і сформулювати основні проблемні питання, які є джерелом такого нерозуміння (див. табл. 1).

Таблиця 1

Перелік факторів та короткий зміст

Фактор ризику	Відомості про фактор ризику
Низька компетентність і кваліфікація користувачів, відповідальних за ЗІ та КБ, а також їх начальників	Низька компетентність і кваліфікація користувачів, відповідальних за ЗІ та КБ, а також їх керівників. У тому числі в частині усвідомлення того, які можуть застосовуватися різновиди комп'ютерних атак, а отже, не повністю правильне налаштування (не виставлення тієї чи іншої «галочки», або відсутність установки якого-небудь оновлення) в конфігурації засобів ЗІ та КБ може служити «діркою» у всій комплексній системі захисту інформації, незважаючи на те, що в загальному вигляді засоби ЗІ та КБ присутні, встановлені і навіть нібито налаштовані.
Відсутність розуміння у керівників (начальників) складності функціонування ІС і	Ознайомлення з особливостями системи йде поверхово, проте необхідно враховувати, що в роботі з ІС надзвичайно важливим принципом є «проблема ховається в деталях».

високої важливості впливу їх особливостей на взаємозв'язок її елементів	Створюється помилкове відчуття, що автоматизація і функціонування ІС, а також ЗІ та КБ в ній відбувається автономна без участі людини. Як наслідок, відбуваються неправильна організація створення, функціонування і захисту ІС.
Погана робота з навчання, інформування, проведення пропаганди (переконання) користувачів, а також відповідальних за ЗІ в частині ЗІ та КБ	У посадових осіб може скластися враження, що в інших країнах справи в частині ЗІ та КБ йдуть набагато краще, ніж у нашій країні. Однак, це достатньо спірний момент, адже і там існує і відома велика статистика за скоєння комп'ютерних інцидентів.
Нерозуміння принципу ІБ та КБ в ІС «Де ризик – там і настає ризиковий випадок». ІС являє собою складну структуру, в тому числі територіально розподілену, де на віддалених об'єктах різних масштабів і складності виконують свої функції по ІБ та КБ окремі відповідальні за ЗІ та КБ	Під управлінням у одного відповідального по ЗІ може бути більше 100 елементів ІС (інформаційних ресурсів, засобів обчислювальної техніки і т. д.), а в іншого з даної ІС всього лише п'ять, а то й взагалі один. У зв'язку з малим обсягом відповідальності може бути знижена пильність як самого адміністратора безпеки інформації, так і його керівництва, адже «що таке лише один комп'ютер»? Але важливо розуміти, що цей технічний засіб знаходиться в одній глобальної обчислювальної мережі, і якщо отримати несанкціонований доступ до нього, то він може послужить підставою (якимось «плацдармом») для побудови вектору та розвитку комп'ютерної атаки.
Відповідальні за ІБ та КБ можуть мати уявлення тільки про своєму елементі ІС	Відповідальні за ІБ та КБ можуть мати уявлення тільки про своєму елементі ІС, у зв'язку з чим може бути відсутнім розуміння всієї структури в цілому, що всі елементи, які б вони малими і непотрібними не здавалися на перший погляд, є частиною одного цілого.
Віднесення інформації що захищається тільки за формальними ознаками, наприклад, таких як особливі позначки або реквізити	Не варто думати, що треба захищати тільки таємні відомості. В даний час існує безліч методик розвідки, заснованих на зборі інформації з відкритих джерел. Інформація, що не має значення на перший погляд на звичайному ПЕОМ користувача, може згодом допомогою її кореляції та аналізу з інформацією з інших джерел за своєю сукупності стати більш критичною або ж послужити відправною точкою для побудови вектору атаки. Наприклад, знаючи прізвище ім'я по батькові працівника, можна цілеспрямовано звернутися до нього по імені, по батькові в шахрайський листі. Водночас для організації існує багато іншої чутливої інформації, що не входить до переліків критичною, але впливає, наприклад, на престиж, або авторитет організації, її співробітників.
Складність збирання інформації (здійснення атаки) – повинна бути виправдана цінністю інформації»	Якщо дані будуть лежати у відкритому доступі або захищатися в недостатній мірі, коли вистачить і мінімальних витрат на її видобуток, то така інформація буде з більшою вірогідністю збиратися, вкладатися в різного роду сховища і згодом аналізуватися. Однак, якщо ускладнити збирання такої інформації простою забороною застосування відчужуваних носіїв інформації, наприклад, флеш-накопичувачів, то і збір такої інформації стає набагато більш ресурсовитратним і, як наслідок, невиправданим. Адже зовні може здаватися, що всього лише включили непотрібну додаткову настройку засобі ЗІ, але з точки зору атакуючого це може бути підставою для прийняття рішення про скасування атаки або збільшення прикладених ресурсів і часу її проведення. У зв'язку з цим важливо відзначити, що, з одного боку, слід максимально відповідальна ставитися до захисту інформації будь-якого роду, з іншого боку, надмірні вимоги по ІБ та КБ можуть істотно знизити її ефективність. Слід керуватися принципом знаходження оптимуму між зручністю функціонування користувача і захистом інформації.
Уразливості, погрози і навіть успішно здійснений несанкціонований доступ у	Цього супротивника і наслідки його дій не можна сприймати органами чуття у звичному вигляді. Для такого аналізу потрібно вкрай висока експертна кваліфікація, і навіть її може бути

більшості випадків носять «невидимий» характер	недостатньо в умовах, коли порушник видаляє інформацію про свою присутність. А раз не видно ворога, то і не ясно вплив на нього вжитих заходів, адже тут, на відміну від протистояння на класичному полі бою, не видно впливу інженерних загороджень на складність їх подолання противником.
У сучасному світі у вузькому розумінні основи життя людини найчастіше зводяться до обмеженого кола «робота–дім–робота»	Іншими аспектами пізнання життя людина може бути не захоплений, а отже, в даній ланцюжку робота стає базовим елементом буття людини. І якщо, наприклад, відповідальний за ЗІ суто механічно налаштовує засоби ЗІ, але при цьому не бачить сенсу і корисності своєї діяльності, то це суттєво впливає на мотивацію людини, провокує його негативне ставлення до цієї діяльності, а отже, призводить до недобросовісного виконання своїх обов'язків.

З перерахованих вище факторів випливає наступне – відсутність загального і стратегічного бачення ситуації, що в свою чергу не дозволяє правильно розставляти пріоритети. Формуються міркування типу – «Навіщо цей елемент взагалі захищати? Нічого страшного не трапиться, адже це просто звичайний мій комп'ютер, на якому я роблю повсякденну роботу». Але навіть якщо робота працівника не представляється важливим, що в рамках великої серйозної організації малоймовірно, то існує можливість, що в умовах недостатньої захищеності, в майбутньому саме з нього локально-обчислювальної мережі або через відчужуваний носій інформації буде заражений критично важливий елемент ІС.

Вищевикладені питання ведуть до виникнення проблеми, яка виражається в формуванні нерозуміння у користувачів і відповідальних за ІБ та КБ своєї ролі і місця в загальній системі ЗІ, а також утворення в них помилкового почуття програної війни в частині інформаційної безпеки. Все це веде до посилення впливу ЛФ на ЗІ, ІС автоматизують і відповідають за різну діяльність людей.

Тож очевидно виникає запитання: Як зменшити людський ризик? Перелік найкращих практики для адміністратора інформаційної безпеки та кібербезпеки подано на ресурсі [23]. Рекомендації головним чином розроблено і націлені на обізнаність у сфері безпеки та навчання, щоб обслуговуючий персонал, користувачі були на висоті перед загрозами. Але зі зростанням складності атак цього підходу стає недостатньо. Ось чому команди з кібербезпеки рекомендують впроваджувати «управління ризиками, пов’язаними з людським фактором». Управління ризиками для людини слід зосереджувати на результатах, а не лише на дотриманні вимог, та кількісно визначати ризик, пов'язаний з людською поведінкою. Так за даними [24] 2024 рік увійде в історію як рік управління людськими ризиками поняття закріплене як окрема категорія, незалежне від навчання з підвищення обізнаності в галузі безпеки, управління людськими ресурсами обіцяє забезпечити більшу віддачу від інвестицій, ніж будь-яка інша стратегічна ініціатива в галузі безпеки. Чому? Тому що для кіберзлочинців головна перевага лежить на людському рівні: соціальна інженерія, фішинг та інсайдерські загрози становлять найбільший ризик багатомільйонних витоків даних, за даними IBM [25]. І ці загрози погіршуються з кожним днем в епоху штучного інтелекту, згідно з даними Verizon DBIR [26].

Отже, платформа управління персоналом (HRM) має бути розроблена таким чином, щоб зменшувати ризик, починаючи з його найбільшого джерела – соціальної інженерії та фішингу. Ефективна платформа HRM призведе до вимірюваних змін у поведінці, які зменшать ризик, шляхом поєднання виявлення загроз – розпізнавання та повідомлення про фішингові атаки – між реальним та змодельованим середовищами. Інтеграція людської інформації про загрози в стек безпеки дозволяє зупиняти загрози до того, як

вони зможуть поширитися.

Але управління персоналом не повинно обмежуватися соціальною інженерією. Цей підхід, заснований на ризиках, може бути застосований до широкого спектру поведінки, включаючи: зберігання та обмін інформацією; автентифікацію та управління доступом; своєчасні оновлення безпеки; та безпечний перегляд веб-сторінок.

Основні принципи підходу, що базується на ризиках для людини, можна застосувати до всіх цих моделей поведінки за допомогою сповіщень на основі поведінкових сигналів, які запускають реакцію адміністратора, автоматичне пом'якшення наслідків або цілеспрямоване мікронавчання.

Сучасні виклики інформаційної безпеки враховані в ISO 27001:2022 та пропонуються можливості для встановлення відповідного підходу до сучасних умов, таких як віддалена робота та цифрові процеси, але все зводиться до посилення контролю персоналу як важливого компонентом системи управлінні інформаційної безпеки та кібербезпеки [27]. Він допомагає впливати на поведінку співробітників щодо інформаційної безпеки та таким чином забезпечувати безпеку інформації.

Заходи, пов’язані з персоналом, надають компаніям рекомендації, що впливають на підбір працівників, навчають їх поводженню з конфіденційною інформацією та сприяють безпечному поводженню з відповідними правилами. Але завжди залишається одне, щоб надмірний контроль за працівниками не спричинили зворотну реакцію до перевтоми від виконання заходів безпеки. Варто пам’ятати, що люди – найбільший ресурс. Люди залишаються залученими роками. Зміна їхньої поведінки є стійкою. Працівники стають рішенням самої проблеми людського ризику.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отже, у сучасному світі людство зіткнулося з проникненням інформаційних технологій в усі сфери життєдіяльності. І якщо кінцевий продукт, одержуваний на виході з ІС, більш або менш визначений і ясний, то складні процеси внутрішнього функціонування ІС закриті і не зрозумілі для більшості користувачів і відповідальних з ЗІ. Поки людина є користувачем інформаційних (автоматизованих) систем, вона буде безпосередньо впливати і на її захищеність. Нерозуміння особливостей взаємодії елементів і процесів ІС із засобами ЗВ тягне за собою неусвідомлене підвищення загроз інформаційної безпеки, що виникають внаслідок впливу ЛФ.

Зараз ця проблема «невизначеності» користувачів і відповідальних за ЗІ, на наш погляд, не виділяється як окрема важлива проблема, яка потребує глобальних змін у підходах до мінімізації впливу ЛФ.

Пропонується шукати вирішення цієї проблеми в першу чергу в осмисленні користувачами і відповідальними за ЗІ їх внеску у процеси захисту інформації інформаційних систем, у тому числі через інформування, формування належної мотивації, відповідних моральних та морально-політичних якостей суб'єктів. Переконаність користувачів важливої ролі відповідального за ЗІ може сприяти вирішенню проблем ефективності захисту інформації. Разом з тим, цього не досягти без віри відповідальних за ЗІ в свої дії і їх компетентному характер.

Справжня проблема потребує окремого поглибленого та комплексного вивчення. Вирішення даної проблеми дозволить знизити негативний вплив ЛФ на інформаційну та кибербезпеку інформаційних систем.

Підготовка та професійний рівень спеціалістів з інформаційної та кібербезпеки має

відповідати таким вимогам: високий загальноосвітній рівень, широкий спектр технічних знань, навики системного підходу до вирішення завдань, вміння приймати нестандартні, але вірні рішення, знання правових питань, знання основ організації та управління, спеціальні знання в галузі інформаційної безпеки.

Наукова новизна. Набула подальшого розвитку теорія захисту інформації через деталізацію людського фактору, що є психолого-педагогічною проблемою.

Практичне значення отриманого наукового результату дає підставу до удосконалення чисельних рекомендацій із запобіганню витоку конфіденційної інформації та проведення роз'яснювальної роботи з особовим складом про небезпечні наслідки від людського фактору.

Перспективи подальших досліджень. Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні та практичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого її вивчення в різних аспектах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. How Much Time Do People Spend on Their Mobile Phones in 2017? (2017). *Hackernoon.* https://hackernoon.com/how-much-time-do-people-spend-on-their-mobile-phones-in-2017-e5f90a0b10a6
2. Information security: types of threats and methods of their elimination. (2024). *Datami.* https://datami.ee/ua/blog/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya
3. Pugachev, O. I. (2024). Problems of ensuring information security of Ukraine in modern conditions. *Problems of Modern Transformations. Series: Law, Public Administration and Management, (12).* https://doi.org/10.54929/2786-5746-2024-12-02-15
4. Zgurovsky, M. (2000). Problems of information security in Ukraine, ways to solve them. *Legal, Regulatory and Metrological Support of the Information Security System in Ukraine: Scientific and Technical Collection, 1,* 10–14.
5. Ostroukhov, V., & Petryk, V. (2008). To the problem of ensuring information security of Ukraine. *Political Management, 4*(31), 135–141. http://dspace.nbuv.gov.ua/handle/123456789/59848
6. Bodrov, V., & Orlov, V. (1998). *Psychology and reliability: Man in technique control systems.* Moscow: Institute of Psychology of the RAS.
7. Poyda-Nosyk, N., Kálmán, B. G., & Malatyinszki, Sz. (2024). The human factor of information security: Phishing in cybercrime. *Acta Academiae Beregsasiensis. Economics, 6,* 223–234. https://doi.org/10.58423/2786-6742/2024-6-223-234
8. Law of Ukraine. (2017). *On the basic principles of ensuring cybersecurity of Ukraine.* https://zakon.rada.gov.ua/laws/show/2163-19
9. Zanyk, O., & Tkachuk, R. (2020). The influence of the human factor on information security organization systems. *Information Security and Information Technologies: Collection of Abstracts of the IV All-Ukrainian Scientific and Practical Conference of Young Scientists, Students and Cadets,* 21–22.
10. Laboratoriya Kasperskogo: polovina kiberincidentov proishodit iz-za chelovecheskogo faktora. (2017). *Agentstvo mezhdunarodnoj informacii Trend.* https://www.trend.az/business/it/2819279.html
11. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. (2017). *AO Kaspersky Lab.* https://www.kaspersky.com/blog/the-human-factor-in-it-security/#:~:text=against%20cyberattack%20is%20their%20own,IT%20security%20strategy%20at%20risk
12. Levchenko, O. V. (2021). *The system of ensuring the information security of the state in the military sphere: The basics of construction and functioning: A monograph.* Zhytomyr: Publisher of PE "Euro-Volyn."
13. The National Museum of Computing (TNMOC). (n.d.). *Official website.* https://www.tnmoc.org
14. Buryachok, V. L., Korchenko, O. G., & Buryachok, L. V. (2012). Social engineering as a method of intelligence of information and telecommunication systems. *Information Security, 14*(4[57]), 5–11.
15. Kozubtsov, I. M. (2015). On the motivational portrait of participants in cyber confrontation. In *Actual Problems of Development of Science and Technology: Materials of the First International Scientific and Technical Conference* (pp. 208–211). State University of Telecommunications.
16. Kozubtsov, I. M., Kozubtsova, L. M., Zhyvilo, E. O., & Kutsaev, V. V. (2016). On the need to study the motivational characteristics of military personnel when they are allowed to engage in cyber confrontation.

In *Application of Information Technologies in the Training and Activities of Law Enforcement Forces: Collection of Materials of the Scientific and Practical Conference* (pp. 35–36). Kharkiv: National Academy of the National Guard of Ukraine.

17. Kutsaev, V. V., Tereshchenko, T. P., & Kozubtsov, I. M. (2017). Information confrontation in social networks. In *Application of Information Technologies in the Training and Activities of Law Enforcement Forces: Collection of Materials of the Scientific and Practical Conference* (pp. 21–22). Kharkiv: National Academy of the National Guard of Ukraine.
18. Skibun, O. Zh. (2022). Modern ethics as a practical philosophy of cybersecurity. *Modern Information Protection, 4*, 66–70. https://doi.org/10.31673/2409-7292.2022.040011
19. Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *IT Professional, 18*(5), 26–32. https://doi.org/10.1109/mitp.2016.84
20. Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia – Social and Behavioral Sciences, 147*, 424–428. https://doi.org/10.1016/j.sbspro.2014.07.133
21. Decree of the President of Ukraine. (2021). *On the decision of the National Security and Defense Council of Ukraine "On the Information Security Strategy."* https://zakon.rada.gov.ua/laws/show/685/2021
22. Kozubtsova, L. M., Kozubtsov, I. M., Tereshchenko, T. P., & Bondarenko, T. V. (2022). On the cyber security of playing geolocation games by military personnel while staying at departmental critical information infrastructure facilities. *Cybersecurity: Education, Science, Technology, 1*(17), 76–90.
23. How to Reduce Human Risk: Best Practices for Security Teams. (2024). *Hoxhunt.* https://hoxhunt.com/blog/how-to-reduce-human-risk#:~:text=,of%20users%20is%20a%20must
24. Baker, E. (2025). *Human risk management playbook.* Hoxhunt. https://hoxhunt.com/guide/human-risk-management-playbook
25. Prassinos, G. (2024). *IBM report: Escalating data breach disruption pushes costs to new highs.* Source IBM. https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs
26. Data Breach Investigations Report. (2025). *Verizon Business.* https://www.verizon.com/business/resources/reports/dbir/
27. People Controls in ISO 27001. (2022). *ENX Association.* https://www.dataguard.com/knowledge/iso-27001/annex-a/6-people-controls/#:~:text=,employees%20to%20information%20security%20risks

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

Lesya M. Kozubtsova
Candidate of Technical Sciences, Associate Professor,
Head of the Department of Mathematics and Physics
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID: 0000-0002-7866-8575
l.kozubtsova@i.ua

Valerii O. Lishchyna,
Candidate of Technical Sciences, Associate Professor,
Head of the Department of Computer Science,
Lutsk National Technical University, Lutsk, Ukraine
ORCID: 0000-0002-2371-3850
lvaleriy@gmail.com

Igor M. Kozubtsov
Doctor of Pedagogical Sciences, Senior Researcher,
Professor, Department of Computer Science
Lutsk National Technical University, Lutsk, Ukraine
ORCID: 0000-0002-7309-4365
kozubtsov@gmail.com

FROM AWARENESS TO MANAGEMENT: THE CONCEPT OF HUMAN RISKS IN CYBER SECURITY SYSTEMS

Abstract. The authors of the scientific article noted that despite the war in Ukraine, society has adapted to the era of information technology, computerization, and automation, with digitalization encompassing all aspects of human life. The concept of the state in a smartphone is increasingly being implemented in various public services for the population. Social services are actively transforming and are even being applied in the military sphere. However, with the growth of digitalization, there is a need to develop countermeasures to strengthen information and cybersecurity, primarily due to the human factor. The purpose of the article is to study the psychological and pedagogical problem of the human factor in ensuring information security and cybersecurity. Research results. The problem of human risk in professional activity is not new. The human factor, patterns, and individual factors that influence professional activity and its impact on the results of activity have been studied by professional psychology theory. In the age of information technology, the human factor is a source of new, previously unseen threats. As modern practice shows, in hybrid warfare, the enemy obtains up to 90% of information through social engineering, receiving valuable information via social networks (Facebook, Telegram channel, Instagram, WhatsApp, Meta, YouTube) that was transmitted through careless conversations. That is why experienced global cybersecurity teams have been thinking about how to reduce human risk in information systems in order to maintain information protection and cybersecurity. This is how the theory of human risk management began, a concept that is established as a separate category, independent of security awareness training. Human resource management promises to deliver a greater return on investment than any other strategic security initiative. The results of the study clearly show the need to implement “human risk management.” Human risk management should focus on results, not just compliance, and quantify the risk associated with human behavior. The theoretical and practical results obtained in the course of scientific research form the basis for further study of various aspects of this issue.

Keywords: information protection; cybersecurity; human factor; information system; information technologies.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. How Much Time Do People Spend on Their Mobile Phones in 2017? (2017). *Hackernoon.* https://hackernoon.com/how-much-time-do-people-spend-on-their-mobile-phones-in-2017-e5f90a0b10a6
2. Information security: types of threats and methods of their elimination. (2024). *Datami.* https://datami.ee/ua/blog/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya
3. Pugachev, O. I. (2024). Problems of ensuring information security of Ukraine in modern conditions. *Problems of Modern Transformations. Series: Law, Public Administration and Management, (12).* https://doi.org/10.54929/2786-5746-2024-12-02-15
4. Zgurovsky, M. (2000). Problems of information security in Ukraine, ways to solve them. *Legal, Regulatory and Metrological Support of the Information Security System in Ukraine: Scientific and Technical Collection*, *1*, 10–14.
5. Ostroukhov, V., & Petryk, V. (2008). To the problem of ensuring information security of Ukraine. *Political Management*, *4*(31), 135–141. http://dspace.nbuv.gov.ua/handle/123456789/59848
6. Bodrov, V., & Orlov, V. (1998). *Psychology and reliability: Man in technique control systems.* Moscow: Institute of Psychology of the RAS.
7. Poyda-Nosyk, N., Kálmán, B. G., & Malatyinszki, Sz. (2024). The human factor of information security: Phishing in cybercrime. *Acta Academiae Beregsasiensis. Economics*, *6*, 223–234. https://doi.org/10.58423/2786-6742/2024-6-223-234
8. Law of Ukraine. (2017). *On the basic principles of ensuring cybersecurity of Ukraine.* https://zakon.rada.gov.ua/laws/show/2163-19
9. Zanyk, O., & Tkachuk, R. (2020). The influence of the human factor on information security organization systems. *Information Security and Information Technologies: Collection of Abstracts of the IV All-Ukrainian Scientific and Practical Conference of Young Scientists, Students and Cadets*, 21–22.
10. Laboratoriya Kasperskogo: polovina kiberincidentov proishodit iz-za chelovecheskogo faktora. (2017). *Agentstvo mezhdunarodnoj informacii Trend.* https://www.trend.az/business/it/2819279.html
11. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. (2017). *AO Kaspersky Lab.* https://www.kaspersky.com/blog/the-human-factor-in-it-security/#:~:text=against%20cyberattack%20is%20their%20own,IT%20security%20strategy%20at%20risk
12. Levchenko, O. V. (2021). *The system of ensuring the information security of the state in the military sphere: The basics of construction and functioning: A monograph.* Zhytomyr: Publisher of PE "Euro-Volyn."
13. The National Museum of Computing (TNMOC). (n.d.). *Official website.* https://www.tnmoc.org
14. Buryachok, V. L., Korchenko, O. G., & Buryachok, L. V. (2012). Social engineering as a method of intelligence of information and telecommunication systems. *Information Security*, *14*(4[57]), 5–11.
15. Kozubtsov, I. M. (2015). On the motivational portrait of participants in cyber confrontation. In *Actual Problems of Development of Science and Technology: Materials of the First International Scientific and Technical Conference* (pp. 208–211). State University of Telecommunications.
16. Kozubtsov, I. M., Kozubtsova, L. M., Zhyvilo, E. O., & Kutsaev, V. V. (2016). On the need to study the motivational characteristics of military personnel when they are allowed to engage in cyber confrontation. In *Application of Information Technologies in the Training and Activities of Law Enforcement Forces: Collection of Materials of the Scientific and Practical Conference* (pp. 35–36). Kharkiv: National Academy of the National Guard of Ukraine.
17. Kutsaev, V. V., Tereshchenko, T. P., & Kozubtsov, I. M. (2017). Information confrontation in social networks. In *Application of Information Technologies in the Training and Activities of Law Enforcement Forces: Collection of Materials of the Scientific and Practical Conference* (pp. 21–22). Kharkiv: National Academy of the National Guard of Ukraine.
18. Skibun, O. Zh. (2022). Modern ethics as a practical philosophy of cybersecurity. *Modern Information Protection*, *4*, 66–70. https://doi.org/10.31673/2409-7292.2022.040011
19. Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *IT Professional, 18*(5), 26–32. https://doi.org/10.1109/mitp.2016.84
20. Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia – Social and Behavioral Sciences, 147*, 424–428. https://doi.org/10.1016/j.sbspro.2014.07.133
21. Decree of the President of Ukraine. (2021). *On the decision of the National Security and Defense Council of Ukraine "On the Information Security Strategy."* https://zakon.rada.gov.ua/laws/show/685/2021

22. Kozubtsova, L. M., Kozubtsov, I. M., Tereshchenko, T. P., & Bondarenko, T. V. (2022). On the cyber security of playing geolocation games by military personnel while staying at departmental critical information infrastructure facilities. *Cybersecurity: Education, Science, Technology*, *1*(17), 76–90.
23. How to Reduce Human Risk: Best Practices for Security Teams. (2024). *Hoxhunt.* https://hoxhunt.com/blog/how-to-reduce-human-risk#:~:text=,of%20users%20is%20a%20must
24. Baker, E. (2025). *Human risk management playbook.* Hoxhunt. https://hoxhunt.com/guide/human-risk-management-playbook
25. Prassinos, G. (2024). *IBM report: Escalating data breach disruption pushes costs to new highs.* Source IBM. https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs
26. Data Breach Investigations Report. (2025). *Verizon Business.* https://www.verizon.com/business/resources/reports/dbir/
27. People Controls in ISO 27001. (2022). *ENX Association.* https://www.dataguard.com/knowledge/iso-27001/annex-a/6-people-controls/#:~:text=,employees%20to%20information%20security%20risks