КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1102
УДК 004.056:004.4'2:159.9

Рибальченко Олексій Геннадійович
аспірант кафедри управління інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0004-5261-3391
cerateg@gmail.com

ЛЮДСЬКИЙ ФАКТОР У СИСТЕМІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНИХ БАЗ ДАНИХ: СОЦІАЛЬНО-ПОВЕДІНКОВИЙ АНАЛІЗ РИЗИКІВ

Анотація. Стаття висвітлює соціально-поведінкову природу ризиків у безпеці корпоративних баз даних, де людський фактор є визначальним чинником інцидентів. Показано, що поведінкові помилки, прогалини у знаннях, стрес і демотивація породжують вразливості, які обходять формальні політики та технічні засоби. Окреслено ролі працівника як оператора й суб'єкта ухвалення рішень. Хибні налаштування доступів, недбале виконання процедур, затримки у виявленні аномалій і помилки інтерпретації сигналів моніторингу спричиняють витоки й порушення цілісності даних. Розглянуто вплив когнітивного й інформаційного перевантаження, нерівномірності компетенцій і низької довіри до цифрових рішень, що зсувають ризик від технічного до поведінкового виміру. Виокремлено сценарії участі людини як жертви або порушника, а саме соціальна інженерія, зловмисні інсайдери й обхідні практики. На прикладах Capital One, Uber і SingHealth показано, як помилки конфігурації, надмірні привілеї, спільні облікові записи, відсутність MFA та ігнорування процедур ескалюють локальні відхилення до масштабних компрометацій. Описано технічні прояви ненавмисних дій у базах даних – неправильні ACL, хибні правила доступу, неповна валідація параметрів, невиявлені SQL-ін'єкції. Показано, що для інсайдерських загроз дієвими є персоналізовані попередження та поведінкова аналітика з індексами ризику, інтегровані з політиками DLP й обмеженням доступу. Розглянуто рамку контрзаходів: принцип найменших привілеїв і багаторівневий захист (defence-in-depth, Zero Trust), безперервний моніторинг IAM/API, регулярний пошук помилкових конфігурацій, сегментацію і контроль привілейованих облікових записів, а також таргетоване навчання з імітаціями інцидентів та зворотним зв'язком. Зроблено висновок, що стійкість систем зберігання даних визначається не лише технологіями, а й керованістю поведінки персоналу.

Ключові слова: інсайдер; мотивація; вразливості; фішинг; людська помилка.

ВСТУП

Постановка проблеми. У системах захисту корпоративних баз даних типовими джерелами ризиків залишаються дії персоналу, що можуть бути ненавмисними наслідками помилкових рішень або порушення встановлених процедур, у результаті чого виникають вразливості й інциденти навіть за наявності формальних політик безпеки [1]. Додатково ризики посилюються через соціальну інженерію та фішингові практики, які системно експлуатують недосвідченість працівників та відсутність навичок верифікації електронних комунікацій [2].

Аналіз останніх досліджень і публікацій. У науковому просторі сьогодення представлено значну кількість досліджень, спрямованих на моделювання поведінкових факторів та соціальної інженерії у кібербезпеці, де переважають підходи до ідентифікації інсайдерів, прогнозу ризиків і мінімізації наслідків атак. Так, у дослідженні [3] показано, що саме внутрішні порушники формують самостійний клас джерел ризику, і при цьому

домінує неофіційний доступ до активів організації через повноваження, які персонал отримує формально за посадою. Окремо підкреслено, що алгоритмічні засоби контролю інсайдерів неможливі без типологізації та системного моделювання суб'єктів, носіями ризику. У цьому контексті представлена класифікація моделей і змішаних систем MS (mixed systems – змішані системи), де моделі IM (intent model – модель намірів) і IBM (individual behaviour model – Модель поведінки особистості) відповідають індивідуальній поведінці, CBM (community behaviour model – модель поведінки спільноти) – груповій поведінці, RUM (resource usage model – модель використання ресурсів) – експлуатації ресурсів, зокрема хмарних технологій, а CM (capability model – модель можливостей) – можливостям суб'єкта, тоді як MS інтегрує ці підходи.

У зазначеному дослідженні [4] акцентовано, що соціальна інженерія експлуатує слабкості людини, які поділяються на особистісні та професійні тригери. Особистісні параметри включають наївність, довірливість, схильність до співпереживання і страх, що у поєднанні з невизначеністю ситуації створює високу ймовірність виконання інструкції, вкладеної у фішингове повідомлення. Професійні тригери корелюють з дефіцитом компетенції, невмінням застосовувати знання на практиці, ігноруванням внутрішніх інструкцій та процедур компанії, що через механізм самовпевненості формує хибне уявлення про власну здатність відрізнити легітимний запит від маніпуляції. Коли ці тригери поєднуються, саме людина трансформується у найбільш вразливий елемент системи, і вихідна модель ризику зміщується з технічного виміру у поведінковий, де агентом зміни є не конфігурація засобів контролю, а зміна когнітивних патернів і патернів реагування персоналу.

У статті [5] подано актуальний огляд соціально-інженерних технік, у яких людський фактор виступає основним вектором доступу до систем. Показано, що фішинг, смішинг та вішинг, разом із претекстингом, клонуванням вебсайтів і видаванням себе за довірену особу, ефективні завдяки експлуатації довіри, страху та відчуття невідкладності, тож суто технічні бар'єри не забезпечують достатнього рівня протидії. Стверджується потреба комплексних контрзаходів, які поєднують технічні засоби з освітніми і організаційними політиками, оскільки саме зміна поведінкових патернів персоналу знижує ймовірність успіху атаки.

У роботі [6] психологічна резильєнтність користувачів і зловмисників трактується як здатність зберігати функціональну стійкість і приймати раціональні рішення під технічним та інформаційно-емоційним тиском, що зумовлює її інтеграцію в архітектуру кіберзахисту поряд із технічними шарами контролю. Показано, що когнітивні упередження та емоційне навантаження знижують опірність жертв до фішингу, а цілеспрямовані когнітивні пастки здатні дезорієнтувати й самого зловмисника, коли психосоціальні впливи поєднуються з технічними засобами кіберобману. Автори формалізують багатофакторну модель резильєнтності користувача через індекси обізнаності, емоцій та упереджень і доводять, що тренування з імітаціями інцидентів та зворотним зв'язком підвищують стійкість у реальних сценаріях. Запропоновано також модель дезорієнтації нападника з експонентним ефектом посиленого впливу, що обґрунтовує впровадження техніко-психологічних пасток у корпоративні середовища та соціальні мережі. Попри прогрес, підкреслюється недостатня інтеграція резильєнтності в політики кібергігієни та стандарти, що окреслює розрив між дослідженнями і практикою та потребує системного оновлення навчальних програм і метрик оцінювання.

У науковій праці [7] здійснено огляд тенденцій кіберзагроз в Україні у взаємозв'язку з інституційною спроможністю держави та практиками бізнесу, де підвищення частоти інцидентів супроводжується розширенням поверхні атаки через

цифровізацію послуг і залежність від хмарних сервісів. Узагальнено, що фішингові кампанії і операції зі шкідливим кодом залишаються ключовими векторами проникнення, тоді як атаки на доступність посилюються на тлі інформаційних маніпуляцій. Підкреслено, що ефективність контрзаходів визначається не лише рівнем технологій, а й сформованістю процедур, культури звітування про інциденти і спроможністю до міжвідомчого обміну даними.

Разом із тим, наявні дослідження рідко пропонують широкий огляд, щодо можливих підходів до інтеграції поведінкових і організаційних чинників у контексті безпеки корпоративних систем зберігання даних.

Мета статті. Метою роботи є формування концептуальної рамки соціально-поведінкового аналізу ризиків для корпоративних баз даних, що узгоджує управлінські і технічні рівні у єдиній системі підтримки рішень. Завдання дослідження полягає в ідентифікації ключових людських чинників, формалізації їхнього впливу на інциденти та узгодженні організаційних вимог із повсякденними практиками.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Людський фактор у безпеці корпоративних баз даних (БД) є ключовим джерелом ризиків. Поведінкові помилки, прогалини у знаннях та демотивація персоналу породжують вразливості, що призводять до інцидентів навіть за наявності формальних політик і технічних засобів контролю. У сучасних дослідженнях людський фактор послідовно описується як «слабка ланка» системи захисту через ненавмисні помилки, неуважність, або навіть навмисні дії співробітників [8].

У ролі оператора людина безпосередньо взаємодіє з системами управління базами даних, де навіть одноразове некоректне рішення здатне створити критичну вразливість, зокрема через неправильне налаштування доступів чи недбале виконання процедур. Такі ситуації описуються як типові прояви ненавмисних помилок та недбалості, які обходять технічні бар’єри і призводять до витоків або порушення цілісності інформації. Ризики додатково зростають за умов надмірних привілеїв, використання спільних облікових даних, відсутності багатофакторної автентифікації та нерегулярного моніторингу й аудиту, що підвищує імовірність компрометації.

Як носій знань і учасник ухвалення рішень працівник формує поведінкові патерни взаємодії з технічними засобами, що створює специфічні ризики для БД. Вони проявляються у затримці або хибному розпізнаванні аномалій, помилки інтерпретації сигналів моніторингу, упереджені пріоритети реагування та розриви у зворотному зв’язку між соціальною і технічною підсистемами [9].

У соціотехнічних системах такі зсуви виникають через когнітивне та інформаційне перевантаження, низьку довіру до цифрових рішень, неоднорідність компетенцій і культурні відмінності, що підвищує ймовірність управлінських помилок і ескалації інцидентів.

Поведінку працівників щодо безпеки БД визначають взаємопов’язані чинники [10]. На індивідуальному рівні вирішальне значення мають внутрішня і зовнішня мотивація, сприйнята загроза, відчуття власної ефективності. Також ключову роль відіграє емоційний стан, наприклад, стрес, що виникає через надмірні вимоги безпеки і може підштовхувати до порушень без прямого наміру. Формальні санкції і винагороди працюють не завжди позитивно, оскільки працівники нерідко приховують провину і узгоджують поведінку з вимогами організації, що призводить до розриву між дотриманням вимог на папері і поведінкою у щоденній роботі.

У ролі порушника чи жертви людина потрапляє під дію соціальної інженерії (social engineering), інсайдерських мотивів та сценаріїв саботажу, де маніпуляція довірою, фішингові повідомлення і навмисне зловживання повноваженнями обходять технічні бар'єри й використовують організаційні прогалини. Такі загрози потребують постійного навчання персоналу, прозорого розмежування обов'язків та регулярних перевірок відповідності, аби виявляти слабкі місця безпеки у БД.

Людей як загрозу для безпеки корпоративних баз даних, поділяють на ненавмисних, недбалих та зловмисних інсайдерів. Причому зловмисний інсайдер чітко відокремлений за ознакою сформованого наміру завдати шкоду заради власної користі, політичних, фінансових або інших мотивів [11].

Ненавмисні помилкові дії у корпоративних базах даних формуються як наслідок того, що технічні середовища з великою кількістю параметрів і точок конфігурації створюють високу ймовірність ненавмисного хибного налаштування. У сучасних хмарних застосуваннях існують сотні технічних точок керування і тисячі конфігураційних параметрів. Саме це збільшує ймовірність того, що адміністратор або розробник залишить конфігурацію в стані, відкритому для несанкціонованого доступу до даних або API, які може використати зловмисник [12].

Помилки такого типу, для баз даних типово проявляються як неправильні ACL, неправильні правила надання та відкликання доступів (GRANT/REVOKE), неповна валідація параметрів запитів, або невиявлена можливість SQL-ін'єкції там де очікувався параметризований запит. Хоча це не є навмисною дією, відсутність наміру суб'єкта не зменшує здатності зловмисника використати наслідок його помилки, а непомітність помилкової конфігурації дозволяє тримати цю ексфільтрацію непоміченою упродовж тривалого часу.

Узагальнені втрати і наслідки таких помилок масштабно продемонстровано на прикладі інциденту Capital One (2019 р.) [12]. У межах якого було скомпрометовано персональні дані близько 100 млн осіб у США та 6 млн у Канаді. Протягом приблизно 127 днів здійснювалося непомітне зчитування та вивантаження орієнтовно 30 ГБ заявок на кредитні картки з численних S3-сховищ, а частина записів могла бути розшифрована, що охоплювало, зокрема, ідентифікаційні та банківські реквізити.

Сукупний ефект формувався поєднанням уразливостей керування доступом і помилок конфігурації на рівні прикладних та інфраструктурних компонентів, що забезпечило тривалу ексфільтрацію чутливих даних і значні юридичні та репутаційні втрати.

Для мінімізації подібних ризиків у дослідженні [13] було запропоновано системно-орієнтований підхід STAMP (System-Theoretic Accident Model and Processes), за яким темп розгортання хмарних сервісів узгоджується зі зрілістю управління ризиками, а розподіл відповідальності в моделі спільної відповідальності уточнюється з урахуванням зниження складності платформи та пріоритизації усунення вразливостей.

На операційному рівні рекомендується запровадження принципу найменших привілеїв і «захист у глибину», посилення ролі наглядової ради та CISO в прийнятті рішень щодо кіберризиків, регулярні огляди безпеки застосунків і процесів керування вразливостями, активний моніторинг подій IAM/API та періодичний пошук помилкових конфігурацій. Застосування цих заходів орієнтоване на зменшення імовірності повторення інцидентів та обмеження їхнього масштабу в разі виникнення.

Недбалість у корпоративному середовищі пов'язана з тим, що залучена особа не дотримується процедур безпеки. Але не через відсутність знань, а тому що для неї доступність і зручність мають вищу суб'єктивну вагу. Наприклад, дослідження

поведінки користувачів показує, що вони здійснюють прямий або варіантний повтор використаних паролів у колективно використовуваних акаунтах, оскільки це полегшує доступ іншим учасникам групи, навіть розуміючи що це зменшує загальний рівень захисту облікових даних [14].

Також у корпоративній БД недбалість проявляється як залишення облікових матеріалів у відкритому вигляді, поширення облікових даних у чатах або копіювання дампів за межі контрольованого середовища. Це не є помилкою конфігурації у вузькому інженерному сенсі, але така поведінка формує додаткову поверхню атаки для зловмисників.

Так, у межах інциденту Uber (у вересні 2022 р.) після первинного доступу через VPN облікові дані було віднайдено у скриптах на мережевому ресурсі, зокрема, виявлено жорстко вшиті привілейовані облікові дані адміністратора до системи PAM (Privileged Access Management) [15].

Отримані на цій підставі права адміністрування були використані для подальшого бічного переміщення всередині корпоративного IT-середовища (lateral movement). Завдяки чому зловмисником було отриманно підвищених дозволів у внутрішніх сервісах: AWS, GCP, Google Drive, Slack, SentinelOne, HackerOne admin console, внутрішні панелі співробітників, репозиторії коду.

Компанія підтвердила завантаження внутрішніх повідомлень Slack, а також доступ до внутрішнього фінансового інструмента для керування окремими інвойсами. У статті окремо зафіксовано, що вшиті облікові дані не ротувалися тривалий час, що спростило їх експлуатацію. Сукупність цих чинників сформувала конкретні наслідки у вигляді доступу до конфіденційних внутрішніх ресурсів і фактичної ексфільтрації службової інформації.

Запропоновані в публікації рекомендації адресують установлені причини інциденту і спрямовані на їх усунення. Вилучення hard-coded секретів, впровадження принципу найменших привілеїв і надання тимчасових прав за запитом зменшують можливості бічного переміщення. Багаторівневий захист у межах Zero Trust разом із навчанням щодо фішингу та методів обходу MFA протидіє соціальній інженерії. Очікуваний результат полягає у зменшенні радіусу ураження та масштабів наслідків у разі повторення аналогічного сценарію.

Інша недбала поведінка полягає у тому, що у корпоративному середовищі процедури контролю доступу, погоджувальних ланцюгів або політик, сприймаються як перепони, що сповільнюють роботу. На емпіричних даних поведінкових опитувань зафіксовано, що обхід процедур розглядається працівниками як локально раціональна імпровізація, спрямована на досягнення результату за умов дефіциту часу або ресурсів.

Але така імпровізація призводить до неконтрольованих обходів політик і формує уразливості, які не перебувають у полі зору заходів безпеки [16]. У таком сценарії, захист не здатний виявити те що відбулося поза процедурою, а отже не здатний створити реалістичний стан «вичерпного» контролю.

У 2018 р. це було емпірично продемонстровано на кейсі SingHealth. В якому саме обхід процедур сприяв тому, що декілька проміжних подій, які окремо виглядали локальними та незначними, не були підняті на вищий рівень реагування та не були розглянуті в контексті єдиного ланцюга компрометації [17].

Унаслідок цього неконтрольований обхід формальних вимог до фіксації і звітності зрештою дозволив зловмисному втручанню залишитись невиявленим майже рік. Завдяки чому у фінальній фазі був отриманий доступ до медичних записів 1,5 млн пацієнтів, включно з VIP-профілями. Це перетворило проблему “зекономленого часу на

узгодження" у збитки на рівні національної системи медичної інформаційної інфраструктури та супроводжувалося накладенням регуляторних штрафів: SGD 750 тис. для IHiS і SGD 250 тис. для SingHealth (разом SGD 1 млн).

У відповідь було рекомендовано відмовитися від периметрової моделі та перейти на багаторівневий захист (defence-in-depth). Це передбачає контроль привілейованих облікових записів, сегментацію для обмеження латерального руху зловмисника, а також розгорнути засоби класу EDR для оперативного виявлення та стримування інцидентів.

Усвідомлена й цілеспрямована інсайдерська злочинна поведінка для корпоративних баз даних, є особливо небезпечою, тому що суб'єкт має доступ до БД, знання внутрішньої структури і точне розуміння де знаходяться критичні дані. Отже атакує не через помилку і не через недбалість, а через раціональний розрахунок вигоди, з приводу цього такий сценарій вимагає окремих контрольних контрзаходів.

У дослідженні [18] було показано на даних великого академічного медцентру США, що інсайдерське "підглядання" в електронні медичні записи не є поодинокими інцидентами. Якщо їх не зупиняти, працівники схильні повторювати несанкціоновані доступи, створюючи для установи фінансові, репутаційні та клінічні ризики. У дослідженні було використано систему моніторингу доступів, для оперативного виявлення порушень серед 444 співробітників протягом 2018 р.

Ключовим управлінським кроком було миттєве індивідуальне попередження електронною поштою в ніч порушення (без негайних дисциплінарних дій, аби не спотворювати результат): 219 порушників отримали такий лист, 225 слугували контрольною групою. Результат – різке падіння повторних інцидентів: 2% (4 особи) проти 40% (90 осіб), що автори інтерпретують як ≈95% ефективність превентивного попередження щодо недопущення повторних доступів.

Додатково зафіксовано 326 повторних порушень у контролі (з них 27% – уже в перші 10 днів) проти поодиноких випадків у групі попереджених. Середній рівень несанкціонованих доступів на працівника становив 1,02 vs 2,45 відповідно. Після завершення експериментального періоду до всіх ідентифікованих порушників було застосовано дисциплінарні заходи, а сам механізм попереджень залишився постійним елементом контролю доступів.

У свою чергу, в дослідженні [19] наведено верифіковані на реальних клієнтських інцидентах кейси зловмисної інсайдерської ексфільтрації, де технічні ознаки подій, часові маркери та міри реагування детально пов'язані між собою. Зокрема, зафіксовано сценарії, коли працівники з керованих пристроїв масово переносили корпоративні файли з OneDrive до особистих хмарних сховищ.

У одному випадку здійснено понад 2,180 завантажень із подальшим вивантаженням 465 файлів у персональний Google Drive, з яких 37 спрацювали за політиками DLP (Data Loss Prevention – запобігання втраті даних). У іншому – близько 2,400 файлів завантажено за 12 днів до звільнення, причому понад 1,500 збіглися з чутливими шаблонами DLP. Кожне з цих відхилень автоматично інкрементувало ризик у User Confidence Index (UCI), переводячи суб'єкта з «безпечної» зони (≈998) у «помірну» (≈562) або навіть «критичну» (≈147), що безпосередньо запускало узгоджені дії контролю доступу.

Саме поєднання Advanced UEBA (поведінкова аналітика та скоринг ризику), DLP та різних політик у реальному часі, таких як двоетапна аутентифікація, обмеження доступу та нормалізація ризикових сигналів через Cloud Risk Exchange, створює керований контур виявлення, ескалації та стримування. Цей контур не лише фіксує факт

ексфільтрації, а й операційно зменшує шкоду за рахунок своєчасного блокування подальшого витоку й дисциплінування користувача.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Людський фактор є головним джерелом ризиків для безпеки корпоративних БД: від ненавмисних помилок і недбалості до цілеспрямованих інсайдерських дій. Ризики посилюють когнітивне перевантаження, надмірні привілеї, спільні облікові записи, відсутність MFA та нерегулярний моніторинг. Кейс-аналіз (Capital One, Uber, SingHealth) і емпіричні дані доводять, що локальні відхилення швидко ескалують у масштабні інциденти. Ефективні контрміри, являють собою поєднання принципу найменших привілеїв, багаторівневий захист та Zero Trust, безперервного IAM/API-моніторингу, регулярного пошуку помилкових конфігурацій, сегментації, контролю привілейованих доступів, а також таргетованого навчання й операційних попереджень.

Подальші дослідження доцільно спрямувати на розробку формалізованих моделей оцінювання поведінкових ризиків у системах захисту корпоративних баз даних, інтеграцію методів машинного навчання та поведінкової аналітики для прогнозування інсайдерських загроз, а також на емпіричну перевірку ефективності Zero Trust і DLP-механізмів у реальних корпоративних середовищах. Перспективним є також вивчення впливу організаційної культури, мотивації персоналу та цифрової грамотності на рівень кіберстійкості організацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Maslova, Yu. Yu., & Kushnir, I. M. (2020). Information security and the human factor. *Modern Information Security, 4*. https://doi.org/10.31673/2409-7292.2020.044145
2. Dovhan, O., Lytvynova, L., & Dorohykh, S. (2023). Cybersecurity in the information society: Information and analytical digest (Issue 9). Kyiv: State Research Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine; Vernadsky National Library of Ukraine. https://ippi.org.ua/sites/default/files/2023-9.pdf
3. Shevchenko, S., Zhdanova, Yu., Skladannyi, P., & Boiko, S. (2022). Insiders and insider information: Essence, threats, activities, and legal responsibility. *Cybersecurity: Education, Science, Technique, 3*(15), 175–185. https://doi.org/10.28925/2663-4023.2022.15.175185
4. Yakymenko, Yu. M., Rabchun, D. I., & Zaporozhchenko, M. M. (2021). The role of social engineering in data leakage issues and organizational aspects of protecting corporate environments from phishing attacks via email. *Cybersecurity: Education, Science, Technique, 1*(13), 6–15. https://csecurity.kubg.edu.ua/index.php/journal/article/view/278
5. Zhmurko, O. (2024). Social engineering as a cybersecurity threat: Prevention and protection methods. *Security Pedagogy, 9*(1), 37–42. https://doi.org/10.31649/2524-1079-2024-9-1-037-042
6. Dzhalladova, I. A.-k., & Kaminskyi, O. Ye. (2025). Socio-psychological resilience of cybersecurity systems. *Modern Information Technologies in the Sphere of Security and Defense, 53*(2), 43–50. https://doi.org/10.33099/2311-7249/2025-53-2-43-50
7. Oniushchenko, S. V., & Hlushko, A. D. (2022). Analytical dimension of cybersecurity in Ukraine under increasing challenges and threats. *Economy and Region, 1*(84), 13–20. https://doi.org/10.26906/EiR.2022.1(84).2540
8. Kras, A. (2025). Human factor and security management. In *Audit of information security: Methodology and practical cases*. In *Problems of Computer Science, Software Modeling, and Security of Digital Systems* (pp. 123–125). https://apcssm.vnu.edu.ua/index.php/conf/article/view/237
9. Kashkanova, A. A. (2025). Socio-technical approach as a way to improve the security environment in urban transport systems. *Bulletin of Vinnytsia Polytechnic Institute, 4*, 170–178. https://doi.org/10.31649/1997-9266-2025-181-4-170-178

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 non-compliance to compliance. *Applied Sciences, 11*(8), 3383. https://doi.org/10.3390/app11083383
11. Ruohonen, J., & Saddiqa, M. (2025). What do we know about the psychology of insider threats? In *Digital Forensics and Cyber Crime (ICDF2C 2024)* (pp. 186–211). https://doi.org/10.1007/978-3-031-89363-6_11
12. Mitchell, B. S., Mancoridis, S., & Kashyap, J. (2024). On the automatic identification of misconfiguration errors in cloud-native systems. In *Proceedings of the 2024 7th Artificial Intelligence and Cloud Computing Conference (AICCC 2024)* (pp. 539–548). https://doi.org/10.1145/3719384.3719463
13. Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A systematic analysis of the Capital One data breach: Critical lessons learned. *ACM Transactions on Privacy and Security, 26*(1), 1–29. https://doi.org/10.1145/3546068
14. Moh, P., Yang, A., Malkin, N., & Mazurek, M. L. (2024). Understanding how people share passwords. In *Proceedings of the Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (pp. 219–237). https://www.usenix.org/conference/soups2024/presentation/moh
15. Sharma, U., & Kalekar, S. M. (2024). Dissecting the Uber security breach: Root cause analysis and mitigation strategies. *International Journal of Computer Engineering and Technology, 15*(4), 715–720. https://doi.org/10.5281/zenodo.13368425
16. Njenga, K., Nyamandi, N. F., & Segooa, M. A. (2024). A model on workarounds and information security integrity. *South African Journal of Information Management, 26*(1), 1–10. https://doi.org/10.4102/sajim.v26i1.1853
17. Ee, S. K. K. (2022). *Prevention is no cure: A case study of the 2018 SingHealth breach*. Digital Asia Hub. https://www.kas.de/documents/288143/14393910/4.1+Prevention+is+No+Cure.pdf
18. Jiang, J. X., Culbertson, N., & Bai, G. (2022). Effectiveness of email warning on reducing hospital employees' unauthorized access to protected health information: A nonrandomized controlled trial. *JAMA Network Open, 5*(4), e227247. https://doi.org/10.1001/jamanetworkopen.2022.7247
19. Netskope. (2023). *Netskope advanced UEBA case studies*. https://www.netskope.com/wp-content/uploads/2023/05/advanced-ueba-case-studies.pdf

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Oleksii Rybalchenko
PhD student of the Department of Information and Cybersecurity Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0004-5261-3391
cerateg@gmail.com

THE HUMAN FACTOR IN CORPORATE DATABASE SECURITY: A SOCIO-BEHAVIORAL RISK ANALYSIS

Abstract. The article highlights the socio-behavioral nature of risks in corporate database security, where the human factor is a determining contributor to incidents. It is shown that behavioral errors, knowledge gaps, stress and demotivation generate vulnerabilities that circumvent formal policies and technical controls. The roles of the employee as operator and decision-maker are outlined. Misconfigured access rights, negligent execution of procedures, delays in anomaly detection and errors in interpreting monitoring signals lead to data leaks and integrity violations. The impact of cognitive and information overload, heterogeneous competencies and low trust in digital solutions is examined, as factors that shift risk from a purely technical to a behavioral dimension. Scenarios of human participation as either victim or offender are identified, namely social engineering, malicious insiders and workaround practices. Case studies (Capital One, Uber and SingHealth) demonstrate how configuration errors, excessive privileges, shared accounts, the absence of MFA and non-compliance with procedures escalate local deviations into large-scale compromises. Technical manifestations of unintentional actions in databases are described: incorrect ACLs, erroneous access rules, incomplete parameter validation and undetected SQL injection. It is shown that, for insider threats, effective measures include personalized warnings and behavioral analytics with risk indices integrated with DLP policies and access restrictions. A countermeasure framework is considered: the principle of least privilege and defence-in-depth (including Zero Trust), continuous IAM/API monitoring, regular search for misconfigurations, segmentation and privileged account control, as well as targeted training with incident simulations and feedback. It is concluded that the resilience of data storage systems is determined not only by technologies, but also by the controllability of personnel behavior.

Keywords: insider; motivation; vulnerabilities; phishing; human error.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Maslova, Yu. Yu., & Kushnir, I. M. (2020). Information security and the human factor. *Modern Information Security*, *4*. https://doi.org/10.31673/2409-7292.2020.044145
2. Dovhan, O., Lytvynova, L., & Dorohykh, S. (2023). Cybersecurity in the information society: Information and analytical digest (Issue 9). Kyiv: State Research Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine; Vernadsky National Library of Ukraine. https://ippi.org.ua/sites/default/files/2023-9.pdf
3. Shevchenko, S., Zhdanova, Yu., Skladannyi, P., & Boiko, S. (2022). Insiders and insider information: Essence, threats, activities, and legal responsibility. *Cybersecurity: Education, Science, Technique, 3*(15), 175–185. https://doi.org/10.28925/2663-4023.2022.15.175185
4. Yakymenko, Yu. M., Rabchun, D. I., & Zaporozhchenko, M. M. (2021). The role of social engineering in data leakage issues and organizational aspects of protecting corporate environments from phishing attacks via email. *Cybersecurity: Education, Science, Technique, 1*(13), 6–15. https://csecurity.kubg.edu.ua/index.php/journal/article/view/278
5. Zhmurko, O. (2024). Social engineering as a cybersecurity threat: Prevention and protection methods. *Security Pedagogy*, *9*(1), 37–42. https://doi.org/10.31649/2524-1079-2024-9-1-037-042
6. Dzhalladova, I. A.-k., & Kaminskyi, O. Ye. (2025). Socio-psychological resilience of cybersecurity systems. *Modern Information Technologies in the Sphere of Security and Defense, 53*(2), 43–50. https://doi.org/10.33099/2311-7249/2025-53-2-43-50

7. Oniushchenko, S. V., & Hlushko, A. D. (2022). Analytical dimension of cybersecurity in Ukraine under increasing challenges and threats. *Economy and Region, 1*(84), 13–20. https://doi.org/10.26906/EiR.2022.1(84).2540
8. Kras, A. (2025). Human factor and security management. In *Audit of information security: Methodology and practical cases*. In *Problems of Computer Science, Software Modeling, and Security of Digital Systems* (pp. 123–125). https://apcssm.vnu.edu.ua/index.php/conf/article/view/237
9. Kashkanova, A. A. (2025). Socio-technical approach as a way to improve the security environment in urban transport systems. *Bulletin of Vinnytsia Polytechnic Institute, 4*, 170–178. https://doi.org/10.31649/1997-9266-2025-181-4-170-178
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 non-compliance to compliance. *Applied Sciences, 11*(8), 3383. https://doi.org/10.3390/app11083383
11. Ruohonen, J., & Saddiqa, M. (2025). What do we know about the psychology of insider threats? In *Digital Forensics and Cyber Crime (ICDF2C 2024)* (pp. 186–211). https://doi.org/10.1007/978-3-031-89363-6_11
12. Mitchell, B. S., Mancoridis, S., & Kashyap, J. (2024). On the automatic identification of misconfiguration errors in cloud-native systems. In *Proceedings of the 2024 7th Artificial Intelligence and Cloud Computing Conference (AICCC 2024)* (pp. 539–548). https://doi.org/10.1145/3719384.3719463
13. Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A systematic analysis of the Capital One data breach: Critical lessons learned. *ACM Transactions on Privacy and Security, 26*(1), 1–29. https://doi.org/10.1145/3546068
14. Moh, P., Yang, A., Malkin, N., & Mazurek, M. L. (2024). Understanding how people share passwords. In *Proceedings of the Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (pp. 219–237). https://www.usenix.org/conference/soups2024/presentation/moh
15. Sharma, U., & Kalekar, S. M. (2024). Dissecting the Uber security breach: Root cause analysis and mitigation strategies. *International Journal of Computer Engineering and Technology, 15*(4), 715–720. https://doi.org/10.5281/zenodo.13368425
16. Njenga, K., Nyamandi, N. F., & Segooa, M. A. (2024). A model on workarounds and information security integrity. *South African Journal of Information Management, 26*(1), 1–10. https://doi.org/10.4102/sajim.v26i1.1853
17. Ee, S. K. K. (2022). *Prevention is no cure: A case study of the 2018 SingHealth breach*. Digital Asia Hub. https://www.kas.de/documents/288143/14393910/4.1+Prevention+is+No+Cure.pdf
18. Jiang, J. X., Culbertson, N., & Bai, G. (2022). Effectiveness of email warning on reducing hospital employees' unauthorized access to protected health information: A nonrandomized controlled trial. *JAMA Network Open, 5*(4), e227247. https://doi.org/10.1001/jamanetworkopen.2022.7247
19. Netskope. (2023). *Netskope advanced UEBA case studies*. https://www.netskope.com/wp-content/uploads/2023/05/advanced-ueba-case-studies.pdf

Отримано редакцією журналу / Received: 27.01.26
Прорецензовано / Revised: 18.02.26
Схвалено до друку / Accepted: 26.03.26