МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

(ПТІКІ'2026)

Одеса, Україна, 16 липня 2026 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ (ПТІКІ'2026)

Матеріали

IV Міжнародної конференції

16 липня 2026 р.

Одеса - 2026

УДК 004.9
П 27

Проведення заходу зареєстровано в Державній науковій установі «Український інститут науково-технічної експертизи та інформації» (Реєстраційний номер: 3326U000765 від 01-07-2026 р.).

Рецензенти:
Надія КАЗАКОВА – д.т.н., професор, завідувач кафедри інформаційних технологій Одеського національного університету ім. І.І. Мечнікова
Віктор СТРЕЛЬБИЦЬКИЙ – к.т.н., доцент, доцент кафедри підйомно-транспортні машини та інжиніринг портового технологічного обладнання Одеського національного морського університету

Передові технології в інформаційно-комунікаційній інженерії (ATICE'2026) : матеріали IV міжнар. конф. (м. Одеса, Україна, 16 липня 2026 р.) / від. за вип.: Н. Пунченко, Д. Розенвассер. Одеса : Міжнар. ун-т, 2026. 149 с. DOI: https://doi.org/10.32837/11300.33747

Advanced Technology in Information and Communication Engineering (ATICE'2026) : proceedings of the IV International conference (Odesa, Ukraine 16 July 2026) / Responsible for the issue: N. Punchenko, D. Rozenvasser. Odesa : International University, 2026. 149 p**.** DOI: https://doi.org/10.32837/11300.33747

У збірнику подано результати наукових досліджень, висвітлено обговорення актуальних проблем, викликів і тенденцій з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами у різних галузях народного господарства. Матеріали охоплюють інноваційні підходи, досвід упровадження сучасних рішень і приклади успішних практик трансформації різних галузях народного господарства .

Видання призначене для науково-педагогічних працівників, здобувачів освіти, науковців і фахівців ІТ галузі.

Відповідальні за випуск:
к.т.н., доцент Пунченко Наталія,
к.т.н., доцент Розенвассер Денис.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова

КІВАЛОВ С.В. – д.ю.н., проф., Міжнародний університет, м.Одеса, Україна.

Співголови

ГРОМОВЕНКО К.В. – д.ю.н., проф., Міжнародний університет, м. Одеса, Україна.
ЛЕФТЕРОВ В.О. – д.п.н., проф., Міжнародний університет, Одеса, Україна
СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., НТУ України "КПІ імені Ігоря Сікорського", Київ, Україна.

Члени організаційного комітету

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ЙОНА Л.Г. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РУСУ О.П. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ВАКАРЧУК А.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ГРІБОВА В.В. – к.ф.-м.н., доц., Міжнародний університет, Одеса, Україна.

РЕДАКЦІЙНИЙ КОМІТЕТ

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний університет, Одеса, Україна.
ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
ГЛОБА Л. С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ВЧЕНИЙ СЕКРЕТАР

ПУНЧЕНКО Н.О. – к.т.н., доц., Міжнародний університет, Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний університет, м.Одеса, Україна.
УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.
ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ЗМІСТ

СЕКЦІЯ 7.
ПСИХОЛОГІЯ ЦИФРОВОГО ПРОСТОРУ. КІБЕРПСИХОЛОГІЯ

УДК 159.9:343.37:004

DOI: https://doi.org/10.32837/11300.33786

ЦИФРОВІ СЛІДИ ДЕСТРУКТИВНОЇ ПОВЕДІНКИ: ПСИХОЛОГІЧНІ ПРЕДИКТОРИ ТА ІНТЕЛЕКТУАЛЬНА ДЕТЕКЦІЯ КОРПОРАТИВНОГО ШАХРАЙСТВА

Гайдуков Ігор Валентинович
аспірант кафедри психології
Міжнародний університет, м. Одеса, Україна

Анотація. *Стрімка цифровізація бізнес-процесів змінює не лише способи здійснення корпоративного шахрайства, а й можливості його раннього виявлення. У роботі запропоновано концептуальну модель, що інтегрує психологічне профілювання співробітників із аналізом цифрових поведінкових слідів у корпоративних інформаційних системах. Теоретично обґрунтовується можливість того, що врахування рис Темної тріади як диспозиційних чинників дозволяє знизити рівень хибнопозитивних спрацьовувань сучасних аналітичних систем. Окреслено специфічні патерни цифрової активності для різних деструктивних профілів та визначено етико-правові межі застосування інтегрованих моделей безпеки.*

Ключові слова: Темна тріада, корпоративне шахрайство, цифрові сліди, поведінкова аналітика, UEBA, ERP, машинне навчання.

Постановка проблеми. Функціонування організацій в умовах тотальної цифровізації супроводжується безперервним формуванням масиву даних про взаємодію користувачів із ERP-системами, корпоративною поштою та базами даних. Наявні інструменти поведінкової аналітики (User and Entity Behavior Analytics (UEBA)) активно фіксують аномалії цифрової активності для виявлення інсайдерських загроз. Проте базовим обмеженням таких систем є те, що вони реєструють виключно наслідки (технічні відхилення від базового профілю - baseline), але не враховують причини (внутрішні психологічні диспозиції особистості). Це призводить до високого рівня хибнопозитивних спрацьовувань (False Positives), коли легітимні, але нестандартні дії лояльного співробітника маркуються як загроза. Виникає наукова задача: інтегрувати психометричні предиктори особистісного ризику з технологіями інтелектуального аналізу даних для підвищення точності проактивних систем детекції шахрайства.

Аналіз останніх досліджень. Провідним конструктом у дослідженні контрпродуктивної робочої поведінки є Темна тріада особистості (макіавеллізм,

нарцисизм, психопатія) [1, 2]. Паралельно технологічний сектор розвиває алгоритми машинного навчання для аналізу часових і операційних аномалій в IT-інфраструктурі [3]. Проте міждисциплінарні дослідження, які пов'язують латентні деструктивні риси із конкретними архітектурними патернами поведінки всередині корпоративного софту, залишаються фрагментарними.

Мета дослідження - обґрунтувати концептуальну модель інтеграції психометричних індикаторів Темної тріади та цифрових поведінкових слідів у єдину систему превентивного ризик-менеджменту корпоративного шахрайства.

Виклад основного матеріалу. Запропонована концепція ґрунтується на тому, що деструктивні риси особистості виступають модераторами стилю взаємодії людини з цифровим робочим середовищем. Комп'ютерний інтерфейс і віддалена робота створюють ефект онлайн-дезінгібіції (розгальмування) [4], знижуючи суб'єктивне сприйняття ризику та полегшуючи раціоналізацію неетичних дій.

Основний принцип запропонованої концепції полягає в тому, що психологічні характеристики не детермінують конкретні шахрайські дії безпосередньо. Вони визначають стиль взаємодії людини з цифровим середовищем, який проявляється у вигляді стійких поведінкових патернів. Саме ці патерни, а не психологічні тести чи окремі дії користувача, є об'єктом аналізу інтелектуальних систем детекції.

Спираючись на психологічні особливості компонентів Темної тріади, можна висунути гіпотезу про існування специфічних стилів цифрової поведінки, які потенційно можуть проявлятися у корпоративних інформаційних системах.

1. Макіавеллізм. Особи з високим рівнем макіавеллізму орієнтовані на стратегічне досягнення власних цілей шляхом прихованого маніпулювання середовищем. У цифровому просторі це може проявлятися як послідовне прагнення до розширення власних можливостей впливу на інформаційні процеси. Потенційними поведінковими індикаторами можуть бути систематичне накопичення прав доступу (privilege escalation), поступове освоєння суміжних функціональних областей інформаційної системи, підвищений інтерес до даних, що безпосередньо не належать до службових обов'язків, а також тривалі підготовчі дії, які самі по собі не порушують політики безпеки, але формують передумови для майбутніх зловживань.

2. Психопатія. Психопатичні риси пов'язані зі зниженою чутливістю до можливих наслідків власних дій, імпульсивністю та схильністю до прийняття ризику. У цифровому середовищі це може проявлятися через ігнорування встановлених процедур інформаційної безпеки, виконання потенційно небезпечних операцій без достатньої перевірки, використання нетипових сценаріїв роботи із системою, різкі зміни поведінкових патернів, а також підвищену варіативність дій порівняно з індивідуальним базовим профілем користувача.

3. Нарцисизм. Для нарцисичних осіб характерними є прагнення до

домінування, потреба у визнанні та демонстрації власної значущості. У корпоративному цифровому середовищі це потенційно може проявлятися не стільки у взаємодії із технічними системами, скільки у специфіці цифрових комунікацій: домінуванні в інформаційному просторі організації, обході формальних каналів взаємодії, демонстративному привласненні результатів колективної роботи, активному просуванні власних досягнень у корпоративних сервісах та підвищеній конфліктності текстових комунікацій, що часто передує інсайдерському зливу даних або саботажу як помсті за невизнання.

Практична реалізація моделі потребує дворівневого архітектурного підходу. Психометричні дані, отримані під час планового HR-асесменту, є конфіденційними й етично не можуть завантажуватися в алгоритми автоматизованого моніторингу для прямого стеження. Замість цього вони формують апріорну ймовірність ризику для конкретної корпоративної ролі чи профілю посади. Коли система UEBA фіксує операційну аномалію, інтегрований аналітичний модуль співвідносить це попередження із рівнем психологічного ризику позиції. Це дозволяє динамічно перераховувати індекс загрози та відсіювати хибні тривоги без порушення норм етики й законодавства про захист персональних даних.

Висновки. Інтеграція психометрії Темної тріади та поведінкової аналітики цифрових слідів трансформує корпоративну безпеку з реактивної (факт аудиту) у проактивну (оцінка динамічного ризику). Подальші дослідження будуть спрямовані на емпіричну валідацію зв'язків між суб'єктивними психометричними профілями та об'єктивними логами інформаційних систем із дотриманням суворих юридичних протоколів комплаєнсу.

Література

1. Paulhus D. L., Williams K. M. The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy. Journal of Research in Personality. 2002. Vol. 36(6). P. 556–563.
2. LeBreton J. M., Shiverdecker L. K., Grimaldi E. M. The dark triad and workplace behavior. Annual Review of Organizational Psychology and Organizational Behavior. 2018. Vol. 5. P. 387–414.
3. Al-Mhiqani M. N. et al. Cyber-Security Incidents: A Review of AI-Based Detection and Mitigation Approaches for Insider Threats. IEEE Access. 2023. Vol. 11. P. 45312–45330.
4. Suler J. The online disinhibition effect. CyberPsychology & Behavior. 2004. Vol. 7(3). P. 321–326.

Інформаційне видання

ЗБІРНИК МАТЕРІАЛІВ

Четвертої міжнародної конференції

«Передові технології в інформаційно-комунікаційній інженерії»

Fourth International Conference

“Advanced Technology in Information and Communication Engineering”

(ATICE'2026)

16 липня 2026 року

Відповідальні за випуск: *Д. М. Розенвассер*, *Н. О. Пунченко*
Комп’ютерний набір і верстка *Н. О. Пунченко*
Редактор *Н. О. Пунченко*
Технічні редактори: *І. В. Новітська, Т. М. Стефанчишена*

Підп. до друку 31.08.2026 р. Об’єм електрон. даних 7,18 Мбайт.

Міжнародний університет м. Одеса
Фонтанська дорога 33, Одеса,