МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ
Навчально-науковий інститут управління, економіки та бізнесу
GDAŃSK UNIVERSITY OF TECHNOLOGY

МАУП

Матеріали
III Міжнародної науково-практичної конференції

“ІННОВАЦІЙНІ МЕТОДИ УПРАВЛІННЯ ЕКОНОМІКОЮ В УМОВАХ ЦИФРОВІЗАЦІЇ БІЗНЕСУ”

10 жовтня 2025 р.

Київ
2025

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ:

Голова оргкомітету:
Гончаренко Михайло Федорович – віцепрезидент Міжрегіональної Академії управління персоналом, д-р екон. наук, проф.

Заступники голови:
Семенець-Орлова Інна Андріївна — директор Навчально-наукового ін-ту управління, економіки та бізнесу, д-р наук з держ. упр., проф.;
Каліна Ірина Іванівна — заступник директора Навчально-наукового ін-ту управління, економіки та бізнесу, д-р екон. наук, проф.

Члени оргкомітету:
Братусь Ганна Анатоліївна — завідувач кафедри управління бізнесом ННІУЕБ, д-р екон. наук, проф.;
Дмитренко Геннадій Анатолійович — почесний професор кафедри економіки бізнесу ННІУЕБ, д-р екон. наук, проф.;
Кришталь Галина Олександрівна — завідувач кафедри фінансів, банківської та страхової справи ННІУЕБ, д-р екон. наук, проф.;
Кривоберець Марина Миколаївна — завідувач кафедри організації туристичної діяльності ННІУЕБ, канд. екон. наук, доц.;
Мазур Юлія Володимирівна — декан ННІУЕБ, канд. екон. наук, доц.

Схвалено Вченою радою Міжрегіональної Академії управління персоналом (*протокол № 9 від 29.10.25*)

ІІІ Міжнародна науково-практична конференція "Інноваційні методи управління економікою в умовах цифровізації бізнесу": зб. матеріалів конференції (м. Київ, 10 жовтня 2025 р.) / ред. кол.: І. А.Семенець-Орлова (гол. ред.), І. І.Каліна (заст. гол. ред.), Ю. В. Мазур (упоряд. і відп. ред.) та ін. Київ: Міжрегіональна Академія управління персоналом, 2025. 512 с.

ISBN 978-617-02-0419-6 (електронне видання)

Для науковців, представників бізнесу та здобувачів вищої освіти.

Тексти тез надано в авторській редакції. Автори несуть повну відповідальність за зміст публікацій, а також добір, точність наведених фактів, цитат, власних імен та інших відомостей.

ISBN 978-617-02-0419-6

© Міжрегіональна Академія управління персоналом, 2025

Привалова Анастасія Валентинівна
Впровадження цифрових технологій як шлях підвищення ефективності організації сільського зеленого туризму в Закарпатській області 471

Собченко Анастасія Володимирівна
Туристично-рекреаційні ресурси Івано-Франківської області 474

Луньова Тетяна Сергіївна
Маркетингова цінова політика транснаціональних корпорацій у сфері електронної комерції 476

Несходовський Ілля Сергійович
Стратегічне управління процесами відновлення на базі Big Data та ШІ: предиктивне моделювання ризиків та оптимізація соціально-економічного мультиплікативного ефекту 479

Скрипцов Святослав Валерійович
Концепція екологічного маркетингу в контексті сталого розвитку 483

Грігєрман Євген Вікторович
Стратегії маркетингу у будівельній галузі в умовах глобальних технологічних змін 486

Чуб Ірина Вікторівна
Національна стійкість як основа національної безпеки 489

Сліпчук Юрій Андрійович
Зарубіжний досвід адміністративно-правового забезпечення розбудови електронного врядування 492

Попов Андрій Вячеславович, Коваль Микола Іванович
Вплив соціальної поляризації суспільства України на формування стратегій цифрового маркетингу 494

Riabovolyk Tetiana Fedorivna, Shevchenko Anna Yuriyivna
Mechanisms of public management in the development of education within the territorial community: experience and prospects for enhancing administrative efficiency 498

Домрачов Андрій Павлович
Бренд-маркетинг аудиторських компаній з використанням цифрових інструментів 501

Жуляєв Владислав Валерійович
Культура захисту даних та оцінювання її рівня в організаціях 503

Vsevolod Koshel, Inna Zhuk
Digital transformation as a catalyst for sustainable growth in the renewable energy industry 506

Черушева Галина Батрбеківна
Поведінкові тригери у маркетингових комунікаціях: як емоції керують вибором споживача 509

сному управлінню потенціалом організації, формуванню довіри, диференціації на ринку та довготривалому зростанню. Для українських аудиторських компаній, що прагнуть інтегруватися у глобальні професійні мережі, ці підходи є особливо актуальними в умовах конкуренції, цифрової трансформації та потреби у прозорості.

Література

1. American Marketing Association. Definition of Brand [Електронний ресурс]. Режим доступу: https://www.ama.org/the-definition-of-marketing/
2. *Аакер Д.* Управління брендовим капіталом. Нью-Йорк: Free Press, 1991.
3. *Салліван Джеффрі.* Створення успішних B2B-брендів. Нью-Йорк: Portfolio, 2009.
4. Deloitte Insights. Human Capital Trends [Електронний ресурс]. 2023. Режим доступу: https://www2.deloitte.com/us/en/insights/focus/human-capital-trends/2023/future-of-workforce-management.html

ЖУЛЯЄВ Владислав Валерійович

аспірант кафедри менеджменту
Міжрегіональної Академії управління персоналом (МАУП, м. Київ)

КУЛЬТУРА ЗАХИСТУ ДАНИХ ТА ОЦІНЮВАННЯ ЇЇ РІВНЯ В ОРГАНІЗАЦІЯХ

Культура захисту інформації в організаціях і на підприємствах (в тому числі захисту персональних даних) є одним із основних факторів захисту даних в системі інформаційної безпеки. Людина (працівник, зокрема і колишні працівники) в більшості випадків є першопричиною внутрішніх порушень інформаційної безпеки та конфіденційності баз даних. Поведінка працівників, яка призводить до багатьох інцидентів безпеки та порушень конфіденційності, є наслідком недбалості, помилки або навмисної зловмисної атаки. Варто зазначити, що поведінка працівників може бути джерелом загрози порушень як для інших працівників, так і для клієнтів організації / підприємства. Дослідники класифікують поведінку працівників за чотирма критеріями: поведінка, яка спрямована на захист безпеки, поведінка, яка відповідає вимогам безпеки, поведінка ризикова для безпеки, поведінка спрямована на порушення безпеки [Guo, 2013].

Саме ці дві останні категорії працівників і становлять пряму загрозу для захисту інформації та призводять до порушень конфіденційності. З огляду на цю проблему департаментам з управління персоналом необхідно зосередитись на культурі захисту інформації та культурі приватності серед працівників, що передбачає донесення знань щодо внутрішніх політик конфіденці-

йності і захисту інформації, регулярне навчання працівників розпізнаванню загроз і методам захисту, запобіганню витоку інформації та порушенню конфіденційності в компанії.

Дослідники приходять до висновків, що необхідною мірою забезпечення захисту інформації в цілому та захисту персональних даних в системі управління персоналом є моніторинг розвитку культури захисту інформації/культури приватності з метою підтримання належного рівня та удосконалення. Моніторинг може здійснюватись за допомогою інших організацій (зовнішній аудит), а також і за допомогою різних шаблонів, на які організації можуть посилатися під час проведення самооцінок, зокрема: чеклісти відповідності GPPR, Data mapping (картування даних) розроблених комісіями із захисту даних окремих країн ЄС, Transfer Impact Assessment (TIA) при передачі даних за межі ЄС, Data Protection Impact Assessment (DPIA) — оцінка впливу на захист даних при маштабних обробках даних, систематичних обробках або впровадженню нових технологій, Керівні принципи оцінки впливу на конфіденційність Управління уповноваженого з питань інформації Сполученого Королівства (ICO 2014) тощо.

Рівень обізнаності працівників організації також можна оцінити за допомогою опитувальників. Однією із методик, яка була використана в якості інструмента оцінки культури інформаційної безпеки на підприємстві є "Оцінка культури інформаційної безпеки" (ISCA), яка була розроблена і випробувана в польових дослідженнях [Da Veiga, Martins, 2015]. Методика є гібридом концепцій організаційної культури та інформаційної безпеки з метою оцінки культури інформаційної безпеки, тобто ставлення до системи спільних базових припущень, цінностей, переконань, норм і правил поведінки, які засвоюються членами організації, передаються новим співробітникам і впливають на те, як організація сприймає, мислить і реагує на внутрішні та зовнішні проблеми та тріаду "CIA" (конфіденційність, цілісність, доступність). Ця тріада встановлює три базові властивості, які необхідно захищати (ISO/IEC 27001: Міжнародний стандарт із систем управління інформаційною безпекою).

Питання ISCA були спеціально розроблені для оцінки ставлення та сприйняття відповідно до структури культури інформаційної безпеки і складалися з 50 питань. Зокрема, одне з оцінювань було застосоване для транснаціональної фінансової компанії, яка здійснює діяльність в 12 країнах світу і проводилося протягом чотирьох років серед більш ніж 2300 працівників методом анкетування з 2010 по 2013 роки. Серед опитуваних працівників дві третини не обіймали керівні посади, решта — менеджери, менше 3 % були керівниками.

Результати дослідження виявили, що працівники, які пройшли навчання з інформаційної безпеки, більш свідомо ставляться до конкретних дій по захисту інформації, вважають важливим обмеження збору та обміну конфіденційною особистою інформацією. Цікавим також є той факт, що 52 % працівників зазначили, що їм не було б комфортно, якщо роботодавець стежив за їхніми публікаціями в соціальних мережах або притягували до відпові-

дальності за публікації про компанію. Близько 47 % працівників компанії скептично поставились до можливості збереження даних про клієнтів, які обробляються третіми особами від імені компанії, що є важливим, оскільки такі порушення можуть призвести до крадіжки особистих даних, шахрайства, відмивання грошей, витоків даних, штрафів регуляторних органів та, зрештою, вплинути на репутацію організації у разі порушення.

Висновки

Термін "інформаційна конфіденційність" часто використовується для позначення належного збору та обробки персональної інформації [Swire & Bermann, 2007]. Є важливим, щоб принципи конфіденційності також були вбудовані в культуру інформаційної безпеки, щоб належним чином обробляти ы зберыгати персональны даны персоналу, а також допомогати у дотриманні вимог та задоволенні очікувань клієнтів під час обробки персональної інформації. Таким чином, культура в організаціях повинна сприяти захисту інформації з точки зору інформаційної безпеки, приватносты та конфіденційності. Це допоможе мінімізувати ризик інцидентів, спричинених працівниками через недбалість, помилку чи навмисні зловмисні атаки під час обробки конфіденційної або персональної інформації.

Таким чином система управління персоналом має бути спрямована на підвищення знань і практик щодо обробки працівниками приватної та конфіденційної інформації у всіх форматах та категоріях протягом її життєвого циклу безпечним способом. Їхню поведінку можна спрямовувати за допомогою таких аспектів, як політики та вимоги до оброблення інформації, включаючи окремі положення про конфіденційність інформації, про захист персональних даних, навчання та підвищення обізнаності, моніторинг, а також сприяння розвитку сильної культури захисту інформації.

Література

1. *Guo C. D.* Research on Enterprise Technology Innovation Mode Selection and Development Path. Ph.D. *Thesis, Beijing Institute of Technology*. 2013. P. 124–139.
2. *Swire P.* Information privacy: official reference for the Certified Information Privacy Professional (CIPP) New York, ME: International Association of Privacy Professionals, 2024.
3. *Da Veiga A., Martins N.* Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*. 2015. Vol. 31. P. 243–256. http://dx.doi.org/10.1016/j.clsr.2015.01.005