

3. PwC Compliance Report re TPB Order dated 25 November 2022
4. Впровадження комплаєнсу на виробничому підприємстві. З чого почати? О. Бажова, експерт-аналітик. URL: <https://salo.li/D4510ba>
5. Комплаєнс-контроль. Що це і навіщо? URL: <https://salo.li/7B0D522>
6. Дзевелюк М., Дзевелюк А., Яременко О. Електронне врядування: приклад впровадження додатку «ДІЯ» в Україні. Наукові перспективи (Naukovі perspektivi). 2023. Вип. 11(25). С. 246-257.
7. Дзевелюк М., Дзевелюк А., Чернищук Н. Цифрові технології і право: виклики цифрової трансформації та кібербезпека. Наука і техніка сьогодні. 2023. Вип 12 (26). С. 62-72.
8. Баймуратов М., Кофман В., Бобровник Д., Дзевелюк М., Дзевелюк А. Analysis of the Practical Aspects of Local Self-Government in the Context of the Functioning of Territorial Communities in Ukraine. Journal of law and sustainable development. Vol. 11. No. 8. 2023. Miami. P. 1-15. ISSN: 2764-4170 <https://ojs.journalsdsg.org/jlss/article/view/1522>
9. Дзевелюк М.В., Дзевелюк А.В. Особливості використання медіації у підготовці юристів та публічних службовців в зво. Міжнародна науково-практична конференція «Медіація & університети 1.0» 15 листопада 2024 р. м. Чернівці. С 113-117.

Динту Анастасія Максимівна

здобувачка ступеня вищої освіти бакалавр
Вінницького державного педагогічного університету
імені Михайла Коцюбинського

Дзевелюк Марина Володимирівна

кандидат юридичних наук, доцент,
доцент кафедри публічного управління та менеджменту
Вінницького державного педагогічного університету
імені Михайла Коцюбинського

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

У сучасних умовах глобалізації та стрімкого розвитку інформаційних технологій питання забезпечення інформаційної безпеки набуває критичного значення. Основними чинниками, що впливають на цю сферу, є: зростання використання цифрових технологій, що робить суспільство залежним від них; широке застосування штучного інтелекту та хмарних сервісів, що створює нові ризики витоку даних; а також воєнні дії на території України, які охоплюють і кіберпростір. Актуальність цієї тематики відображена в наукових дослідженнях таких фахівців, як Бурячок В.Л., Ільїн М.І., Пилипчук В.Г., Андерсон Р., Браун Д., Сміт А. та ін. Проте з огляду на динаміку

розвитку кіберзагроз багато аспектів залишаються відкритими. Зокрема, компанії дедалі частіше впроваджують програми кібергігієни та тренінги з соціальної інженерії для співробітників. Також набуває популярності використання штучного інтелекту для виявлення аномалій і кіберзагроз, що зумовлено зростаючою складністю атак. Водночас людський фактор залишається критичним викликом, оскільки низька цифрова грамотність значно підвищує ризики безпеки.

Інформаційна безпека є невід'ємною частиною національної безпеки, адже всі загрози, що впливають на державу, безпосередньо відображаються в інформаційному просторі. Сучасні соціально-економічні реалії України, а також недоліки в організації державного управління та функціонуванні громадянського суспільства створюють значний спектр внутрішніх загроз для інформаційної безпеки держави [7]. Також інформаційна безпека є основою реалізації функцій публічного управління, оскільки всі напрями державної політики мають бути захищені в умовах сучасного інформаційного суспільства [9, с. 196]. Варто зауважити, що в умовах воєнного стану, постійні атаки країни агресора на українські бази даних, питання кібербезпеки стає вкрай актуальним [4, с. 65].

Законодавче регулювання цієї сфери включає визначення основних компонентів національної безпеки, стратегічних цілей та принципів їх захисту. Інформаційна безпека пов'язана із захистом інформаційного суверенітету держави, що передбачає контроль над інформаційними потоками та захист внутрішньої інформації. Особливої актуальності набуває боротьба з інформаційним впливом, маніпуляціями, фейковими новинами та діяльністю ботів, що спрямовані на дезорієнтацію та дестабілізацію суспільства [6, с. 102].

У міжнародному контексті правове регулювання інформаційної безпеки адаптується до сучасних викликів, спираючись на нормативні акти ООН. Важливим завданням правової науки є аналіз цих принципів та їх інтеграція в національне законодавство [8].

В Україні забезпечення інформаційної безпеки регулюється рядом нормативно-правових актів, серед яких ключову роль відіграє Закон України «Про засади забезпечення кібербезпеки в Україні». Відповідно до нього, кібербезпека визначається як захист кіберпростору та життєво важливих інтересів держави, суспільства й громадян від кіберзагроз через комплекс правових, організаційних, адміністративних і технічних заходів [5].

На міжнародному рівні застосовуються такі технології для забезпечення інформаційної безпеки, які доцільно розглядати й в Україні: *криптографія* – методи шифрування та дешифрування інформації, що забезпечують конфіденційність даних; *автентифікація користувача* – багаторівневі механізми перевірки доступу, включаючи паролі, біометрію та токени; *брандмауери* – програмне забезпечення для контролю доступу до мережевих ресурсів; *захист мережевої інфраструктури* – інструменти безпеки мережі, включаючи контроль доступу та моніторинг загроз [3, с. 289]. Окремо варто згадати *технологію блокчейн*, яка завдяки своїй децентралізованій природі

забезпечує надійний захист даних. Її застосування активно розширюється у фінансовому секторі, охороні здоров'я, управлінні ланцюгами поставок та державному управлінні [2, с. 580].

При цьому, в Україні також можна відмітити успішно функціонуючу платформу «Дія», яка розташована в надійному дата-центрі та відповідає світовим стандартам захисту від кіберзагроз, а усі дані передаються й зберігаються виключно у шифрованому вигляді [4, с.65]. Важливим аспектом розвитку інформаційної безпеки також є *стандартизація*. В Україні необхідно вдосконалювати захист інформаційних систем відповідно до міжнародних стандартів ISO/IEC 27000. Це передбачає оновлення нормативної бази, адаптацію національних підходів до світових практик та інтеграцію механізмів управління ризиками в державних установах [1, с. 66].

Отже, інформаційна безпека є одним з ключових елементів національної безпеки України. Вона потребує комплексного підходу, що включає впровадження передових технологій, посилення кібергігієни та удосконалення законодавства. Важливим завданням є глобальна стандартизація систем кібербезпеки, що сприятиме підвищенню стійкості країни до сучасних викликів цифрової епохи.

Список використаних джерел

1. Артюшин Г., Волощенко А. Шляхи вдосконалення механізмів забезпечення захисту інформації в інформаційно-телекомунікаційних системах СБ України. *Інформаційна безпека людини, суспільства, держави*. 2024. № 1–3 (34–36). С. 64–71.
2. Бондарчук О. І., Гаць Б. М., Осадчук С. І. Використання блокчейн-технологій для забезпечення кібербезпеки в комп'ютерних системах. *Інформаційна безпека людини, суспільства, держави*. 2024. № 1–16 С. 574–589.
3. Виганяйло С. М., Колісник Т. П. Технології захисту інформації та інформаційна безпека. *«Правова наука і державотворення в Україні в контексті інтеграційних процесів»*: матеріали XIV Міжнар. наук.-практ. конф., 19–20 трав. 2023 р. Суми: МВС України, Харків. нац. ун-т внутр. Справ. С. 287–289.
4. Дзевелюк М., Дзевелюк А., Чернишук Н. Цифрові технології і право: виклики цифрової трансформації та кібербезпека. *Наука і техніка сьогодні*. 2023. Вип 12 (26). С. 62-72.
5. Закон України «Про основні засади забезпечення кібербезпеки України» №2163-VIII від 5 жовтня 2017 року. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 10.03.2025).
6. Котляров В. Аналіз сучасного стану інформаційної безпеки в Україні. *Mechanism of an Economic Regulation*. 2024. № 2 (104). С. 101-104. DOI: <https://doi.org/10.32782/mer.2024.104.16>.
7. Панченко О. Інформаційна складова національної безпеки. *Вісник Національної академії Державної прикордонної служби України*. 2019. №3. URL: <https://periodica.nadpsu.edu.ua/index.php/governance/article/view/296/297>.

8. Пугачов О. І. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2024. № 13. DOI: <https://doi.org/10.54929/2786-5746-2024-13-02-07>.

9. Філіпішина Л., Костик Є., Дзевелюк М.В. Публічне управління у сфері інформаційної безпеки (подолання сучасних загроз). *Актуальні питання у сучасній науці*. 2023. Вип. 5 (11). С. 196 – 205.

Довгань Вероніка Олегівна

здобувачка ступеня вищої освіти магістр

Вінницького державного педагогічного університету
імені Михайла Коцюбинського

МОТИВАЦІЙНІ ІНСТРУМЕНТИ ЯК ЗАСІБ ПІДВИЩЕННЯ ВІДКРИТОСТІ ТА ПІДЗВІТНОСТІ ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ У ПРОТИДІІ КОРУПЦІЇ

Забезпечення відкритості та підзвітності органів місцевого самоврядування є важливим фактором ефективної боротьби з корупцією. У сучасних умовах особливої уваги потребують механізми мотивації посадових осіб, які сприяють підвищенню їхньої відповідальності, доброчесності та ефективності роботи. У роботі розглянуто основні мотиваційні інструменти, які можуть застосовуватися для забезпечення відкритості та підзвітності в органах місцевого самоврядування, а також їхній вплив на антикорупційну діяльність.

Корупція залишається однією з ключових проблем у сфері місцевого самоврядування. Відсутність належної підзвітності та низький рівень відкритості сприяють зловживанням владою. Одним із механізмів подолання цих проблем є використання дієвих мотиваційних інструментів, що забезпечують стимулювання посадових осіб до ефективної, прозорої та відповідальної роботи [3].

Мотиваційні механізми можуть суттєво впливати на поведінку працівників органів місцевого самоврядування. Основними їх видами є:

- Матеріальні стимули: конкурентоспроможна заробітна плата, премії за доброчесність, соціальні гарантії.
- Нематеріальні стимули: кар'єрне зростання, суспільне визнання, підвищення кваліфікації.
- Антикорупційні інструменти: запровадження механізмів контролю та моніторингу діяльності посадових осіб [4].

Фінансова мотивація є важливим елементом у боротьбі з корупцією, оскільки недостатній рівень оплати праці є одним із чинників виникнення корупційних ризиків. Водночас, нематеріальні стимули, такі як соціальний