DOI https://doi.org/10.36059/978-966-397-601-3-86

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ

Ірина ШОПІНА
доктор юридичних наук, професор,
професор кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ
м. Львів, Україна

Розуміння класичної структури інформаційної безпеки в науці інформаційного права включає її розгляд на трьох рівнях: загальнодержавному (національному), корпоративному (організаційному, локальному) та особистісному. Кожен з цих рівнів передбачає існування властивих йому ризиків та загроз.

На загальнодержавному рівні інформаційна загроза розуміється як потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні[1]. До таких ризиків та загроз на глобальному рівні відносять збільшення кількості глобальних дезінформаційних кампаній, російську інформаційну політику, соціальні мережі як суб'єкти впливу в інформаційному просторі, недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій. На національному рівні інформаційними загрозами визначено інформаційний вплив держави-агресора на населення України, її інформаційне домінування на тимчасово окупованих територіях України, обмежені можливості реагувати на дезінформаційні кампанії, несформованість системи стратегічних комунікацій, недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів, спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України, доступ до інформації на місцевому рівні, недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії

[1] Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

маніпулятивним та інформаційним впливам[2]. Аналіз сутності вказаних ризиків свідчить, що вплив цифровізації в їх переліку відображений, але розглядається переважно в контексті можливої чутливості до російських інформаційних впливів. Водночас проблема активного впровадження інформаційних технологій має розглядатися, на нашу думку, значно ширше, оскільки сфера взаємодії людини з новітніми інформаційними технологіями несе у собі комплекс ризиків, обумовлених не тільки зовнішньополітичними, а й внутрішніми факторами.

Корпоративний рівень інформаційної безпеки становить цілісну систему стратегічного та технологічного управління, що має на меті захист даних з обмеженим доступом, попередження дестабілізації службової діяльності внаслідок дій в інформаційному просторі, а також захист інформаційних прав і свобод людини, у тому числі її персональних даних. державної таємниці та службових даних. Слід зупинити увагу на існуванні деяких відмінностей корпоративної безпеки державних та комерційних структур. Так, на відміну від комерційних структур, де безпека фокусується на прибутках, у правоохоронних органах вона має державно-центричний характер, оскільки витік інформації безпосередньо загрожує ефективній діяльності такого органу, а за певних умов – національній безпеці. Основою цього рівня є суворе дотримання політик класифікації даних, де чітко розмежовано доступ до відкритої інформації та інформації з обмеженим доступом, а також нормативне затвердження всіх етапів інформаційної діяльності, з властивими останнім обмеженнями. Такі заходи переважно спрямовані на забезпечення кібербезпеки і становлять сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на захист від кіберзагроз, забезпечення кібербезпеки, стійкості, цілісності, доступності та конфіденційності інформаційних ресурсів у кіберпросторі, а також здатності інфраструктури до їх обробки[3]. Кількість кіберінцидентів в Україні дійсно є вражаючою: Національна команда реагування на кіберінциденти CERT-UA у 2025 році опрацювала 5927 кіберінцидентів. Це на 37,4% більше, ніж у 2024 році[4].

Однак слід пам'ятати, що інформаційна безпека значно ширша за своїм масштабом, ніж кібербезпека. Загальновідомо, що найслабшим

[2] Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

[3] Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

[4] CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: які були атаки. URL: https://yur-gazeta.com/golovna/certua-u-2025-roci-opracyuvala-mayzhe-6000-kiberincidentiv-yaki-buli-ataki.html

елементом всіх систем безпеки залишається людина. Не є винятком і системи інформаційної безпеки, в яких саме від дій людини залежить надання несанкціонованого доступу до інформації, оприлюднення без належних на те підстав чутливих відомостей та даних, а також здійснення помилкових професійних дій, які можуть мати своїми негативними наслідками зниження ефективності діяльності організації, порушення прав і свобод людини та громадянина. Тому саме третій, особистісний, рівень є, на нашу думку, найбільш важливим в контексті активної цифровізації, що є нині невід'ємним елементом розвитку всіх сфер суспільних відносин.

Цифрова трансформація – це процес кардинальної перебудови організації, управління, функцій та методів діяльності, інформаційної культури та інформаційної свідомості суб'єктів правовідносин за рахунок використання ними інформаційних технологій. Основні напрями цифрової трансформації включають: а) підвищення ефективності технологічних процесів; б) оптимізацію структури організації, змісту її діяльності та системи підготовки, прийняття та виконання управлінських рішень; в) підвищення рівня інформаційної культури та інформаційної свідомості індивідуальних і колективних суб'єктів, включаючи громадянське суспільство; г) зменшення рівня корупції, суб'єктивності та міжрегіональних бар'єрів у системі публічної служби; г) зменшення частки неефективної рутинної праці у структурі зайнятості завдяки використанню штучного інтелекту; д) створення моделі цифрового розвитку, наслідування якої сприяє більш повному задоволенню потреб та інтересів фізичних та юридичних осіб[5].

Оптимізація структури організації, змісту її діяльності та системи прийняття управлінських рішень передбачає впровадження цифрових платформ, інтегрованих інформаційних систем та міжвідомчого обміну даними. Однак такі процеси супроводжуються ризиками надмірної централізації інформації, що може створювати передумови для зловживань владою або несанкціонованого використання даних. Крім того, автоматизація управлінських рішень може знижувати рівень індивідуальної відповідальності посадових осіб та ускладнювати встановлення причинно-наслідкових зв'язків у разі прийняття помилкових рішень.

Підвищення рівня інформаційної культури та інформаційної свідомості є необхідною умовою ефективної цифровізації, проте цей процес потребує системного навчання, формування цифрових

[5] Шопіна І.М., Грищук А.Б. (2022). Поняття, напрями та суб'єкти цифрової трансформації: правові аспекти. *Правовий часопис Донбасу*. №4. С.167-170. DOI https://doi.org/10.32782/2523-4269-2022-81-4-1-167-170

компетентностей та розвитку критичного мислення. Без належної підготовки персоналу використання сучасних технологій може призводити до їх формального або неефективного застосування, а також до порушень вимог інформаційної безпеки. Крім того, щорічно збільшується кількість випадків впливу на людину з метою отримання доступу до інформаційних ресурсів (фішинг, вішинг (голосовий фішинг), baiting (приманка), pretexting (легенда) тощо)[6].

Зменшення частки рутинної праці завдяки активним процесам цифровізації сприяє підвищенню ефективності діяльності, однак одночасно актуалізує питання трансформації кадрового складу, необхідності перекваліфікації працівників та забезпечення належного рівня людського контролю за автоматизованими процесами. Надмірна автоматизація без належного контролю може створювати загрози порушення прав і свобод людини. На нашу думку, сучасний рівень проникнення інформаційних технологій у всі сфери людської діяльності потребує виокремлення категорії «людський контроль» і застосування вказаної форми контролю як при аналізі процесу діяльності з використанням цифрових інструментів, так і під час аналізу якості її результатів («подвійний людський контроль»).

[6] Шарова Т. М. (2025). Інформаційна безпека в епоху цифрової трансформації. *Інформаційні технології в металургії та машинобудуванні – ІТММ 2025*: матеріали Міжнародної наук.-технічної конференції (Дніпро, 23 квітня 2025 р.). С. 652-656. DOI: 10.34185/1991-7848.itmm.2025.01.117