ГРОМАДСЬКА ДУМКА ПРО ПРАВОТВОРЕННЯ

У НОМЕРІ:

- **КІБЕРБЕЗПЕКА**

  Національні системи реагування на кібератаки

- **ПРАВООХОРОННА СИСТЕМА**

  Повноваження Нацгвардії: розширення чи уніфікація

№ 10 (296) ТРАВЕНЬ 2025

НАЦІОНАЛЬНА БІБЛІОТЕКА УКРАЇНИ ІМЕНІ В. І. ВЕРНАДСЬКОГО
НАЦІОНАЛЬНА ЮРИДИЧНА БІБЛІОТЕКА

ГРОМАДСЬКА ДУМКА ПРО ПРАВОТВОРЕННЯ

№ 10 (296) 2025

Інформаційно-аналітичний бюлетень
на базі оперативних матеріалів

Додаток до журналу
«УКРАЇНА: ПОДІЇ, ФАКТИ, КОМЕНТАРІ»

Засновники:
Національна бібліотека України
імені В. І. Вернадського
Національна юридична бібліотека

Головний редактор
Ю. Половинчак

Редакційна колегія:
Н. Іванова (відповідальна за випуск), Т. Дубас,
Ю. Калініна-Симончук

Заснований у 2011 році
Видається двічі на місяць

З повнотекстовою версією видання можна
ознайомитись на сайті
Центру досліджень соціальних комунікацій
nbuviap.gov.ua

ЗМІСТ

АКТУАЛЬНА ПОДІЯ
22 травня 2023 р. набрав чинності Закон України щодо механізму компенсації за пошкоджене та знищене війною майно.....3

АНАЛІТИЧНИЙ РАКУРС
Чернявська Л.
Національні системи реагування на кібератаки: досвід створення, функціонування та сучасні виклики 4
Кривецький О.
Повноваження Нацгвардії: розширення чи уніфікація 20

ЩОДЕННИК БЛОГЕРА *.....22

Київ 2025

АКТУАЛЬНА ПОДІЯ

22 травня 2023 р. набрав чинності Закон України щодо механізму компенсації за пошкоджене та знищене війною майно

22 травня 2023 р. набрав чинності Закон України № 2923-IX «Про компенсацію за пошкодження та знищення окремих категорій об'єктів нерухомого майна внаслідок бойових дій, терористичних актів, диверсій, спричинених збройною агресією Російської Федерації проти України, та Державний реєстр майна, пошкодженого та знищеного внаслідок бойових дій, терористичних актів, диверсій, спричинених збройною агресією Російської Федерації проти України».

Документ було офіційно опубліковано в газеті «Голос України» 22 березня.

Згідно з документом для розгляду питань щодо надання компенсації за знищені об'єкти нерухомого майна виконавчий орган сільської, селищної, міської, районної у місті (у разі її створення) ради, військова адміністрація населеного пункту або військово-цивільна адміністрація населеного пункту утворює Комісію з розгляду питань щодо надання компенсації за знищені об'єкти нерухомого майна внаслідок бойових дій, терористичних актів, диверсій, спричинених збройною агресією Російської Федерації проти України, як консультативно-дорадчий орган та затверджує положення про роботу такої Комісії.

Заява про надання компенсації за знищений об'єкт нерухомого майна подається до Комісії з розгляду питань щодо надання компенсації, уповноваженої розглядати заяви про надання компенсації за знищені об'єкти нерухомого майна на відповідній території. Така заява подається під час дії воєнного стану та протягом одного року з дня його припинення або скасування на території, на якій розташований (розташовувався) знищений об'єкт нерухомого майна.

Заява про надання компенсації за знищений об'єкт нерухомого майна подається щодо кожного знищеного об'єкта нерухомого майна окремо.

Заява про надання компенсації за знищений об'єкт нерухомого майна може бути подана до Комісії з розгляду питань щодо надання компенсації:

1) в електронній формі – засобами Єдиного державного вебпорталу електронних послуг;

2) у паперовій формі – через центр надання адміністративних послуг, орган соціального захисту населення або нотаріуса.

Компенсація за знищений об'єкт нерухомого майна надається шляхом:

1) надання грошових коштів шляхом їх перерахування на поточний рахунок отримувача компенсації із спеціальним режимом використання для фінансування будівництва будинку садибного типу, садового або дачного будинку. Такий рахунок відкривається на ім'я отримувача компенсації. Порядок відкриття та ведення таких рахунків визначає Національний банк України;

2) фінансування придбання квартири, іншого житлового приміщення, будинку садибного типу, садового або дачного будинку (у тому числі фінансування придбання такого приміщення/будинку, що буде споруджений у майбутньому, або інвестування/фінансування його будівництва) з використанням житлового сертифіката.

Компенсація за пошкоджений об'єкт нерухомого майна надається шляхом виконання робіт, пов'язаних з будівництвом, на пошкодженому об'єкті нерухомого майна з метою його відновлення (у тому числі розроблення проєктної документації на будівництво, проведення її експертизи, виконання будівельних робіт) та/або надання будівельної продукції для виконання таких робіт.

Порядок надання компенсації за пошкоджений об'єкт нерухомого майна визначає Кабінет Міністрів України.

Законом визначено, що в разі смерті отримувача компенсації до спадкоємця (спадкоємців) переходить право на отримання компенсації за пошкоджений/знищений об'єкт нерухомого майна (у тому числі житловий сертифікат) ***(LIGA ZAKON (https://jurliga.ligazakon.net/news/218318_22-travnya-nabrav-chinnost-zakon-shchodo-mekhanzmu-kompensats-za-poshkodzhene-ta-znishchene-vynoyu-mayno). – 2025. – 26.05).***

АНАЛІТИЧНИЙ РАКУРС

Л. Чернявська, наук. співроб., НЮБ НБУВ

Національні системи реагування на кібератаки: досвід створення, функціонування та сучасні виклики

Особливості профільного національного законодавства

Основи національного законодавства у сфері кібербезпеки закладено в Конституції України. Ст. 17 передбачає, що захист інформаційної безпеки є однією з найважливіших функцій держави і справою всього українського народу, а ст. 18 Конституції України вимагає, щоб зовнішньополітична діяльність України була спрямована на забезпечення її національних інтересів і безпеки шляхом підтримання мирного і взаємовигідного співробітництва із членами міжнародного співтовариства за загальновизнаними принципами і нормами міжнародного права.

Згідно зі ст. 106 Конституції України, Президент України відіграє важливу роль у забезпеченні національної безпеки, до якої відноситься і кібербезпека, зокрема як голова Ради національної безпеки і оборони, той, хто відповідає за національну безпеку та оборону і хто вносить до парламенту подання про призначення на посаду та звільнення з посади голови Служби безпеки України.

На момент повномасштабного вторгнення РФ, Україна фактично знаходилася на початковому етапі системної організації боротьби з кіберзлочинністю. Значним кроком стало створення в жовтні 2015 р. кіберполіції, яка функціонує в межах Національної поліції України і спеціалізується на захисті прав і свобод громадян, а також на запобіганні, виявленні та розслідуванні кіберзлочинів.

Із 2016 р., коли була прийнята Стратегія кібербезпеки України, почалася активна розбудова національної системи кібербезпеки. Були створені спеціалізовані центри кіберзахисту у ключових державних установах, таких як: Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національний банк України, Міністерство інфраструктури України, Міністерство оборони України та Збройні сили України.

У жовтні 2017 р. був ухвалений Закон України «Про основні засади забезпечення кібербезпеки України», що визначає правові основи захисту національних інтересів у кіберпросторі. Він встановлює цілі та принципи державної політики у сфері кібербезпеки, повноваження державних органів та інші ключові аспекти.

У 2021 р. було затверджено оновлену Стратегію кібербезпеки України та створено Національний координаційний центр кібербезпеки, що координує діяльність всіх органів у сфері кібербезпеки. Ці заходи доповнюються активною міжнародною співпрацею із країнами ЄС, США, НАТО та іншими партнерами для проведення кібернавчань та обміну передовим досвідом.

У грудні 2024 р. Кабінет Міністрів України затвердив зміни до Положення про організаційно-технічну модель (ОТМ) кіберзахисту. Передбачається впровадження єдиного підходу до забезпечення кіберзахисту інформаційно-комунікаційних систем державних органів та об'єктів критичної

інфраструктури, що ґрунтується на положеннях Cybersecurity Framework 2.0 від NIST (Національного інституту стандартів та технологій США).

В оновленій ОТМ кіберзахисту визначено базові заходи з кіберзахисту:

– Управління ризиками – визначення стратегій та політик для ідентифікації, аналізу й управління кіберризиками.

– Ідентифікація ризиків – оцінка поточних та потенційних загроз для виявлення вразливих місць у системах.

– Захист даних – використання методів і процедур для забезпечення захисту конфіденційної інформації від несанкціонованого доступу та витоку.

– Виявлення загроз – ідентифікація підозрілої активності та кіберінцидентів за допомогою спеціалізованого програмного забезпечення та моніторингу систем.

– Реагування на загрози – впровадження заходів для швидкого реагування на кіберінциденти, запобігання їхньому поширенню та усунення наслідків.

– Відновлення після атак – проведення відновлювальних робіт після кіберінцидентів для повернення систем до штатного режиму роботи та аналіз причин для запобігання повторним атакам.

В оновленій ОТМ кіберзахисту також буде оптимізовано взаємодію суб'єктів кібербезпеки в межах національної інформаційно-комунікаційної системи. Буде сформовано трирівневу взаємозалежну кібербезпекову інфраструктуру.

CSF 2.0 акцентує увагу на можливості організацій не лише запобігати кібератакам, а й швидко адаптуватися до нових загроз. Оновлена версія CSF розроблена для інтеграції з міжнародними та іншими стандартами включно з ISO/IEC 27001, ISO/IEC 27110, SOC 2, NIST RMF, COBIT та ін. У документі вперше окремо розглядаються ризики, пов'язані з новітніми технологіями.

Упровадження CSF 2.0 дасть можливість посилити управління кіберризиками, захист державних інформаційних систем, включно з базовими реєстрами, критичною інфраструктурою тощо, від сучасних кіберзагроз. Це також позитивно вплине на підготовку та ефективне реагування на нові кібератаки та підвищення рівня довіри серед інвесторів і партнерів.

Крім того, впровадження нового стандарту покращить кіберзахист для бізнесу. Тепер і середній, і малий бізнес зможе ефективніше впроваджувати міжнародні практики, користуючись адаптованими рекомендаціями CSF 2.0.

Ці зміни є частиною виконання Стратегії кібербезпеки України та відповідають сучасним викликам у сфері глобальної безпеки.

На стадії розгляду у ВРУ перебуває наразі проєкт закону «Про Кіберсили Збройних Сил України», метою якого є створення військової та технічної організаційної структури у складі Збройних сил України за стандартами НАТО, яка відповідатиме за кібероборону України, захист її суверенітету та територіальної цілісності в кіберпросторі.

Держспецзв'язку та СБУ затвердили нові рекомендації та форму плану захисту від кіберзагроз для об'єктів критичної інфраструктури (ОКІ). Спільний Наказ № 627/772 від 19 грудня 2024 р. встановлює сучасні стандарти кібербезпеки, враховуючи сучасні виклики у сфері інформаційної безпеки. Документ містить оновлені шаблони планів, обов'язкову оцінку ризиків, врахування залежностей між об'єктами інфраструктури та адаптацію до нових загроз. Змінено порядок затвердження планів: тепер вони мають погоджуватися послідовно з Держспецзв'язку та СБУ.

У квітні 2025 р. набув чинності Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» (№ 4336-IX, поточна редакція від 27.03.2025 р.).

Законом передбачається:

– створення та забезпечення функціонування національних систем реагування на інциденти кібербезпеки, кібератаки, кіберзагрози та обміну інформацією про інциденти кібербезпеки щодо інформаційних, електронних,

комунікаційних, інформаційно-комунікаційних та технологічних систем, в яких оброблюються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– розбудова в рамках національної системи реагування команд реагування та визначення ролей і завдань національної, галузевих та регіональних команд реагування з урахуванням рекомендацій, визначених NIS 2 Directive;

– делегування завдань від національного CSIRT (CERT-UA) до галузевих і регіональних команд реагування, а також можливість залучення приватних команд реагування до національної системи реагування;

– визначення ролей та взаємодії суб'єктів реагування в разі настання кризової ситуації в кібербезпеці;

– створення правової основи для запровадження системи оцінювання стану кіберзахисту та запровадження авторизації систем з безпеки, яка поступово замінить існуючу процедуру побудови комплексних систем захисту інформації;

– суттєве вдосконалення процедури створення комплексної системи захисту інформації (зокрема, прибираються непотрібні бар'єри для підтвердження відповідності);

– створення профільних підрозділів з кіберзахисту в державних органах, на об'єктах критичної інфраструктури, а також визначення типових вимог до таких підрозділів та їх керівників;

– проведення систематичних навчань, тренінгів з кіберзахисту та захисту інформації, а також інструктажів з кібергігієни;

– уточнення деяких принципів та пріоритетів розвитку національної системи кібербезпеки тощо.

Таким чином, у державних органах та на об'єктах критичної інфраструктури планують створити профільні підрозділи з кіберзахисту. До складу національної системи реагування на інциденти кібербезпеки входитимуть: CERT-UA, що є національною командою реагування на кібератаки (національний CSIRT), а також галузеві та регіональні команди реагування на інциденти кібербезпеки, кібернапади, кіберзагрози (галузеві та регіональні CSIRT), які створюються державними органами або органами місцевого самоврядування для підвищення ефективності реагування на кіберзагрози в окремих галузях або регіонах. Функціонування цієї системи забезпечуватиме Державна служба спеціального зв'язку та захисту інформації, яка має запровадити систему навчань посадовців з кіберзахисту та захисту інформації, а також інструктажі з кібергігієни.

Ще однією метою Закону, за словами його авторів, є гармонізація українських стандартів зі стандартами Європейського Союзу та НАТО. Одна з ідей нардепів – доповнити Закон України «Про основні засади забезпечення кібербезпеки України» новою статтею «Національна система обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози». Новий Закон гармонізує українське законодавство з європейськими стандартами (NIS 2 Directive), що важливо для інтеграції з ЄС. Він також спрощує бюрократію, замінюючи складну систему Комплексної системи захисту інформації (КСЗІ) на сучасніші підходи до кіберзахисту. За словами члена Комітету ВР з питань цифрової трансформації О. Федієнка, ухвалений документ має імплементувати норми європейських директив з кібербезпеки у національне законодавство, «але з урахуванням національних інтересів».

Стан кібербезпеки в Україні і світі

Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA заявляє про тенденцію до зростання кібератак на критично важливу інфраструктуру. Загалом у 2024 р. фахівці CERT-UA опрацювали 4315 кіберінцидентів. Це на 69,8 % більше, ніж роком раніше, коли кіберзлочинці атакували український кіберпростір 2541 раз. Найчастіше зловмисники атакували місцеві органи влади, уряд та урядові організації, сектор безпеки та оборони, енергетичний сектор, комерційні організації, телекомунікації. Найпоширенішими типами інцидентів були: розповсюдження шкідливого програмного забезпечення, фішинг, шкідливе підключення, компрометація облікового запису або системи.

У березні масштабної кібератаки зазнала «Укрзалізниця». Очевидно, що питома вага кіберзагроз у спектрі загроз національній безпеці країн зростає, і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься.

Національна Стратегія кібербезпеки України (2021 р.) визнає кіберпростір разом з іншими фізичними просторами одним з можливих театрів воєнних дій, тому спроможність держави захищати національні інтереси в ньому розглядається як важлива складова кібербезпеки. Набирає сили тенденція зі створення нового роду військ – кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, спрямованих на знищення обчислювальних мереж та інформаційних систем збройних сил противника, а також виведення з ладу критично важливих об'єктів противника шляхом руйнування інформаційних систем, які управляють такими об'єктами.

Водночас все більш активно застосовується поєднання традиційних та нетрадиційних стратегій і тактик з використанням цифрових інформаційних технологій. Зокрема, Російська Федерація активно реалізує концепцію інформаційного протиборства, базовану на симбіозі бойових дій у кіберпросторі та інформаційних операцій, механізми якої активно застосовуються у процесі гібридної війни проти України. Країни ЄС, НАТО, провідні міжнародні компанії та експерти одностайно визнають її дії у кіберпросторі головною загрозою міжнародній кібербезпеці. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури.

Прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності в кіберпросторі, що проявлятимуться насамперед у розширенні кола держав, які намагатимуться сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувальнопідривної діяльності в кіберпросторі, посилити державний контроль за національними сегментами мережі «Інтернет».

Негативною ознакою технологічного розвитку, пов'язаного із всеохоплюючим поширенням цифрових технологій, розширенням інтернет– середовища, є критично зростаючий технічний рівень інструментарію реалізації кіберзагроз, від чого ландшафт таких загроз охоплює все більше сфер життєдіяльності. Кібератаки, їх різновиди стають все більш інтелектуальними та небезпечними, створюючи реальну загрозу критично важливій інфраструктурі. Масштабу глобального тренда набуває використання кіберпростору терористичними організаціями (кібертероризм). Цьому сприятимуть всеохоплююча цифрова трансформація систем управління та життєзабезпечення, що невпинно розширює цільову аудиторію кібертероризму та спектр потенційних об'єктів кібератак.

Нові виклики несе із собою перехід на 5G-мережі, функціонування яких кардинальним чином залежить від коректної роботи програмного забезпечення, що за рахунок новизни технології може мати нові, не повною мірою передбачені загрози. Технології «інтернет-речей», «розширена реальність», «розумне місто» активно доповнюються новими – «гіпераутоматизація», «розумно компонований бізнес», «кібербезпекова сітка», «розподілена хмара», «інтернет-поведінка» тощо.

Швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища.

Створення національних систем реагування на кібератаки сьогодні є надзвичайно актуальним у контексті нещодавніх атак на сайти об'єктів критичної інфраструктури, державні реєстри та ін. Зокрема, експерт з кібербезпеки й екскерівник центру реагування на кіберзагрози Cert UA К. Корсун наголошує на обмеженому фінансуванні та недостатності кадрового потенціалу системи захисту

від кіберзагроз, що призводить до таких негативних наслідків. Насамперед, зазначає він, бракує людей належної кваліфікації з кіберзахисту. А сама система захисту недостатньо фінансувалася – за залишковим принципом, тобто тими грішми, які залишилися після витрат на цифровізацію, – зазначив К. Корсун. У результаті, незважаючи на досить серйозний захист системи, вона продовжує залишатися недостатньо захищеною. К. Корсун також акцентував увагу на відсутності в Україні окремого центру, який би відповідав за експертизу з кібербезпеки. Ще одним «мінусом» він назвав відсутність сучасного законодавчого регулювання. Однак в Україні, підсумував експерт, відсутній «нормальний» закон щодо кібербезпеки. У нас є кривий і застарілий Закон України «Про основні засади забезпечення кібербезпеки України», куди постійно щось додають. От і Закон України № 4336-IX, на його думку, – це теж Закон про внесення змін до законів, тобто чергові «латки». Це намагання лікувати систему, що не працює. В Україні немає якогось єдиного органу влади, який би відповідав за кібербезпеку. Не тільки брав би гроші на розвиток кібербезпеки, але і відповідав за наслідки, зокрема негативні.

Іншим аспектом, що створює вразливість української системи кібербезпеки є вендорлоки – монополія постачальників послуг. За словами експерта в галузі GovTech, співзасновника компанії Strimco Р. Ланського, монополія постачальників послуг є однією з можливих причин масштабної кібератаки на українські реєстри, що сталася наприкінці минулого року. Багато українських відомств працюють з визначеними підрядниками, які монополізують доступ до систем, як результат – вони не оновлюються і не модернізуються. Така монополія ускладнює контроль за безпекою продуктів. За словами Р. Ланського, деякі компанії створюють сервіси на рідкісних технологіях, на кшталт Elixir, уникають передачі документації або просто блокують доступи для інших підрядників. «Така монополія обмежує можливості для конкуренції, а також може створити середовище для корупційних домовленостей між постачальниками та замовниками. Навіть найсучасніші технології, які використовувалися для розробки систем 15–20 років тому, в сучасних умовах вже не є достатньо ефективними чи безпечними. До того ж, якщо є залежність від компанії, надзвичайно важко змусити її дотримуватись тих чи інших безпекових стандартів», – підкреслив Р. Ланський. За його оцінкою, близько половини державних систем тою чи іншою мірою залежать від монопольних постачальників або конкретних людей, які контролюють системи.

Та незважаючи на певні недоліки і зауваження, цей Закон є важливим для України. Його ухвалення – це відповідь на зростання загроз, зокрема в умовах, коли державні ресурси та критична інфраструктура є головними мішенями хакерів. Цей новий Закон, на думку більшості експертів, закладає сучасну правову основу кібербезпеки, гармонізовану з європейськими підходами (зокрема, імплементує рекомендації директиви NIS2).

Україна поступово розвиває партнерство із приватним сектором у кіберсфері: діють інформаційно-аналітичні центри при критичних підприємствах, запускаються платформи обміну інформацією про кіберзагрози. Нові норми Закону стимулюють співпрацю, дозволяючи залучати бізнес до відсічі кібератак на державу на офіційних засадах. Також Україна робить ставку на підготовку кадрів – у вишах відкриваються спеціальності з кібербезпеки, створюються навчальні центри за підтримки західних партнерів, проводяться кібернавчання (наприклад, регулярні навчання з НАТО).

Провідні країни світу значну увагу приділяють підготовці та ефективності своїх кібервійськ. Щорічно, наприклад, в Ізраїлі, на кібербезпеку виділяється 150 млн дол., а понад 1000 спеціалістів працюють у кіберпідрозділах. Лідером у цій галузі є США, які вкладають 7 млрд дол. на рік і мають приблизно 9 тис. кіберфахівців. Провідні країни реалізують масштабні проєкти з кібербезпеки, спрямовані освітню підготовку своїх громадян: навчальні програми для підготовки спеціалізованих кадрів та інформування громадськості, включаючи навчання школярів навичок цифрового захисту.

Український ринок кібербезпеки за останні 8 років зріс у 4 рази: із 32 млн дол. у 2016 р. до 138 млн дол. у 2024 р. Для порівняння, у Польщі він складав 800 млн дол. у минулому році.

Найбільший приріст ринку спостерігався у 2021 р. – 92 млн дол. або +33 %. У 2022 р. був помірний ріст ринку (105 млн дол.) через релокації компаній та закриття офісів, що призвели до зменшення внутрішнього попиту на кібербезпеку та сповільнення росту інвестицій. У 2023 р. відбулося збільшення до 122 дол.

Світовий ринок кібербезпеки минулого року сягнув 186 млрд дол., частка України складає приблизно 0,07 %. До трійки лідерів входять США (81 млрд дол.), Китай (15 млрд дол.) та Велика Британія (11 млрд дол.).

На українському ринку кібербезпеки переважає сегмент мережевої безпеки, але безпека додатків та кінцевих точок швидко зростають.

Із 2016 р. ринок хмарної безпеки в Україні виріс з 0,1 млн дол. до 1,7 млн дол. у 2024 р. За час повномасштабного він збільшився втричі.

Минулого року ринок мережевої безпеки склав 46,3 млн дол., ринок безпеки кінцевих точок – 7,1 млн дол.

У дослідженні DataDriven Research&Consulting прогнозується, що український ринок кібербезпеки зросте ще на 50 % протягом п'яти років і досягне 209 млн дол.

Таким чином сьогодні кібербезпека стала ключовим напрямом державних політик в усьому світі. Провідні держави створили свої ефективні інституційні моделі і політики у цій сфері.

Міжнародні угоди у сфері кібербезпеки

Хоча кібербезпека є критично важливою сферою, не існує всеосяжного глобального міжнародного договору, який встановлював би міжнародні стандарти. Оскільки кіберпростір – відносно нове явище, глобальні міжурядові установи не прийняли жодних юридично обов'язкових договорів чи конвенцій. Процес переговорів з цього питання триває, та оскільки різні країни використовують різні підходи навіть щодо термінології, він є повільним і складним. У 2011 і 2015 роках Російська Федерація та Китай спробували представити Генеральній Асамблеї ООН «Кодекс поведінки з інформаційної безпеки», однак, його не було прийнято до розгляду. Між Китаєм, РФ та США – так званими «кіберсупердержавами» – існують великі розбіжності щодо регулювання правил у сфері кібербезпеки. Зважаючи на всі нюанси, пов'язані зі складом наведеного списку, шанси на ухвалення зведених договорів у близькому майбутньому доволі низькі.

Частково питання кібербезпеки регулює ***Конвенція ООН проти транснаціональної організованої злочинності (2000),*** яка є глобальним міжнародним договором. Попри те, що в ній конкретно не йдеться про кіберзлочинність, її положення є дуже актуальними, оскільки вона створює правові рамки для екстрадиції, взаємної правової допомоги та співробітництва в правоохоронній сфері. Україна підписала її в 2000 р. і ратифікувала з застереженнями в 2004 р. (цими застереженнями є: 1) «Конвенція застосовуватиметься тільки за умови дотримання конституційних принципів і фундаментальних засад правової системи України»; 2) «термін "тяжкий злочин" відповідає термінам "тяжкий злочин" і "особливо тяжкий злочин" в українському кримінальному законодавстві»).

Ще один глобальний міжнародний документ, який частково регулює питання кібербезпеки, – це ***Статут Міжнародного союзу електрозв'язку*** 1992 р. Цей договір є засадничим документом Міжнародного союзу електрозв'язку (МСЕ) – спеціалізованої установи ООН. Статут було підписано всіма державами-членами ООН, включаючи Україну. Він регулює підтримання та розширення співробітництва щодо використання телекомунікацій на міжнародному рівні; розвиток засобів та ефективність послуг у цій сфері; а також дії, що перешкоджають роботі існуючих телекомунікаційних мереж.

Конвенція про кіберзлочинність Ради Європи (CETS № 185), відома як ***Будапештська конвенція***, є єдиним юридично обов'язковим міжнародним документом з цього питання; у ній зазначено, що це «перша міжнародна угода

щодо злочинів, вчинених через інтернет та інші комп'ютерні мережі, яка стосується, зокрема, порушень авторських прав, пов'язаного з комп'ютерами шахрайства, дитячої порнографії та порушень мережевої безпеки. Вона також містить низку повноважень та процедур, як-от пошук комп'ютерних мереж та перехоплення даних». Будапештська конвенція служить настановою для будь-якої країни, що розробляє всеохоплююче національне законодавство проти кіберзлочинів та основою для міжнародного співробітництва між державами-учасницями цієї угоди. Будапештська конвенція доповнена протоколом щодо «актів ксенофобського та расистського характеру, вчинених через комп'ютерні системи» та Директивною запискою. Будапештська конвенція була ухвалена у 2001 р. та набула чинності у 2004 р. Україна ратифікувала конвенцію у 2005 р., передбачивши деякі важливі застереження до неї, в тому числі щодо того, чи передбачати в національному законодавстві кримінальну відповідальність за виробництво чи використання програм або пристроїв з метою незаконного доступу чи перехоплення даних, а також втручання у дані або систему. Україна залишила за собою право не застосовувати п. 1 ст. 6 Будапештської конвенції, яким передбачено, що «…кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином: і. пристроїв, включаючи комп'ютерні програми, створених або адаптованих, в першу чергу, з метою вчинення будь-якого зі злочинів […]; іі. комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів […]». Під «злочинами» в Будапештській конвенції маються на увазі правопорушення, зазначені в ст.ст. 2–5, а саме, незаконний доступ, незаконне перехоплення даних, втручання в дані та втручання в систему.

15 жовтня 2015 р. Україна заявила, що з 20 лютого 2014 р. і на період тимчасової окупації Російською Федерацією частини території України – Автономної Республіки Крим та міста Севастополь, а також окремих районів Донецької та Луганської областей, тимчасово непідконтрольних Україні, – застосування та виконання Україною зобов'язань за Будапештською конвенцією обмежуються і не гарантуються. Варто згадати, що РФ – єдина європейська країна, яка не підписала Будапештську конвенцію – частково тому, що вона дозволяє іноземним правоохоронцям безпосередньо допитувати провайдерів інтернет-сервісу. РФ офіційно стверджувала, що ратифікація Будапештської конвенції може порушити російський суверенітет. Більше того, РФ планує запропонувати новий пакт ООН про кіберрегулювання, який має стати «кіберкодексом поведінки» та шляхом до нової конвенції про кіберзлочинність. РФ проводить тиху лобістську кампанію на підтримку свого ООНівського пакету, організовуючи та спонсоруючи заходи, присвячені обговоренню кіберзлочинів.

Третій розділ Будапештської конвенції визначає основу міжнародного співробітництва у сфері протидії кіберзлочинам. Коли йдеться про міжнародне співробітництво, Будапештська конвенція передбачає екстрадицію та взаємну правову допомогу. Міжнародне співробітництво щодо екстрадиції частково охоплено ст. 10 Кримінального кодексу України та двосторонніми угодами, підписаними з різними країнами.

6 липня 2016 р. Європейський парламент ухвалив ***Директиву щодо мережевої та інформаційної безпеки*** (Директиву NIS), яка стала першим єдиним для Європейського Союзу законодавчим актом щодо кібербезпеки. Вона передбачає правові заходи, спрямовані на різке підвищення загального рівня кібербезпеки в ЄС через забезпечення ефективних операцій Групи реагування на інциденти, пов'язані з комп'ютерною безпекою (CSIRT або CERT), та компетентного органу у сфері мереж та інформаційних систем, інтенсифікацію міжнародного співробітництва і встановлення

культури дотримання вимог щодо безпеки та інформування відповідно до Директиви NIS. Директива NIS доповнена Інструментарієм NIS (NIS Toolkit) – інформацією, що має на меті підтримати державичлени ЄС в їхніх спробах реалізувати Директиву NIS швидко й узгоджено в усьому ЄС. В Інструментарії наведені найкращі практики, пояснення та тлумачення.

Оскільки Україна не є частиною ЄС, Директива NIS не є для неї юридично обов'язковою, однак, вона є керівним принципом щодо належної практики. Хоча деякі положення були добровільно введені в українське законодавство.

Зарубіжний досвід регулювання питань кібербезпеки

США

Сполучені Штати Америки мають одну з найрозвиненіших законодавчих баз у сфері кібербезпеки. Існує низка законів і актів Конгресу, що визначають політику: від Акту про кібербезпеку 2015 р. (що спростив обмін інформацією про загрози) до щорічних оборонних бюджетів, які включають кіберположення. У 2023 р. адміністрація оприлюднила нову Національну стратегію кібербезпеки США, яка зміщує акцент на проактивний захист критичної інфраструктури і спільну відповідальність держави та бізнесу за кіберстійкість. Важливу роль відіграють також укази Президента США: зокрема, Указ № 14028 (травень 2021 р.) «Про поліпшення кібербезпеки нації» посилив вимоги до безпеки федеральних мереж та запровадив обов'язкові стандарти (наприклад, нульова довіра, мультифакторна автентифікація тощо).

У США діє розгалужена система органів кібербезпеки з розподілом за функціями:

– Агентство з кібербезпеки та безпеки інфраструктури (CISA) при Міністерстві внутрішньої безпеки – головний цивільний орган, відповідальний за захист національної критичної інфраструктури та координацію зусиль в кіберсфері. CISA виступає координатором загальнодержавних зусиль з кіберзахисту критичних секторів, забезпечує моніторинг загроз, реагування на інциденти, розробку стандартів і рекомендацій. Через CISA реалізується модель Sector Risk Management Agencies – 16 секторів критичної інфраструктури закріплені за профільними міністерствами, які у співпраці з CISA опікуються кібербезпекою у своїх галузях (наприклад, за енергетику відповідає Міністерство енергетики, за фінанси – Мінфін і т.д.).

– ФБР – веде розслідування кіберзлочинів, контррозвідку в кіберпросторі та реагує на кібератаки терористичного/державного характеру, тісно взаємодіючи з CISA і приватними компаніями.

– Кіберкомандування США (USCYBERCOM) при Міністерстві оборони – відповідає за воєнні кібероперації та захист військових мереж.

– Агентство національної безпеки (NSA) – окрім розвідки, має Центр кібербезпеки для співпраці з промисловістю (Cybersecurity Collaboration Center) і спільно з CISA та іншими допомагає захищати оборонно-промисловий комплекс.

– Офіс національного директора з кібербезпеки (ONCD) в Білому домі – нова структура (створена у 2021 р.) для стратегічної координації кіберполітики на найвищому рівні та контролю виконання Національної кіберстратегії.

Оскільки значна частина критичної інфраструктури США знаходиться у приватній власності, партнерство держави і бізнесу є наріжним каменем політики. Ще з початку 2000-х років діє модель публічно-приватного партнерства: створено численні платформи обміну інформацією про кіберзагрози, такі як ISAC (Інформаційно-аналітичні центри) у різних секторах (фінансовий, енергетичний, транспортний тощо). CISA відіграє роль моста між урядом та бізнесом: організовує регулярні брифінги, випускає попередження і рекомендації, проводить спільні навчання з компаніями. Національна кіберстратегія (2023) прямо зазначає необхідність колективного захисту, де уряд допомагає компаніям захищатися, а компанії діляться з урядом інформацією про інциденти. Для зручності обміну даними CISA розгорнула систему автоматизованого сповіщення про загрози

(наприклад, платформа Automated Indicator Sharing). Також при CISA діє програма Joint Cyber Defense Collaborative (JCDC) – спільний центр планування захисту за участі провідних ІТ-корпорацій, телекомів і урядових агенцій.

США інвестують значні ресурси в розвиток кіберкадрів. Національна ініціатива з освіти у сфері кібербезпеки (NICE) під егідою NIST формує стандарти професійних навичок. Існує програма CyberCorps: Scholarship for Service, яка надає стипендії студентам кібертехнологічних спеціальностей за умови подальшої роботи в уряді. Агентство CISA розвиває навчальні курси, проводить кібернавчання для штатів і приватних партнерів. Важливою є робота з молоддю: кіберпатріотичні змагання (CyberPatriot для школярів), університетські центри академічної досконалості (CAE) у співпраці з АНБ, освітні програми в коледжах. У цілому, формується екосистема освіти: від шкільних гуртків до програм магістратури з кібербезпеки та сертифікації фахівців (CISSP тощо).

Велика Британія

Велика Британія системно підходить до кібербезпеки, оновлюючи стратегію кожні п'ять років. Остання Національна кіберстратегія Великої Британії (2022–2030 рр.) визначає пріоритети: зміцнення стійкості критичних секторів, розвиток технологічного лідерства та нарощування навичок. На законодавчому рівні ключову роль відіграють Правила безпеки мереж та інформаційних систем (NIS Regulations 2018) – британська імплементація європейської директиви NIS, яка зобов'язує операторів критичної інфраструктури (енергетика, транспорт, охорона здоров'я тощо) впроваджувати заходи кібербезпеки і повідомляти про інциденти. Після Brexit Британія зберігає ці норми та планує оновити їх відповідно до NIS2. Окремі закони посилюють захист суміжних сфер: наприклад, Акт про телекомунікації (Telecommunications Security Act 2021) ввів суворі вимоги до безпеки 5G-мереж, а Акт про безпеку продуктів та телеком-інфраструктури (2022) регулює кібербезпеку IoT-пристроїв. Каркас кримінального права у кіберсфері задає ще старий Акт про неправомірне використання комп'ютерів 1990 року, проте, його також переглядають для актуалізації.

Центральним вузлом британської моделі є Національний центр кібербезпеки (NCSC) – експертний орган, створений у 2016 р. у складі розвідслужби GCHQ. NCSC став єдиною точкою контакту з кібербезпеки для бізнесу, уряду і суспільства. По суті, він поєднав раніше розрізнені структури (CERT-UK, CESG) і взяв на себе координацію реакції на інциденти та консультаційну підтримку. NCSC захищає критичні системи та мережі Великої Британії від кібератак, діючи «містком» між індустрією та урядом. Центр надає рекомендації з найкращих практик, реагує на кіберінциденти (допомагає жертвам атак відновитися, координує розслідування з поліцією), випускає попередження про загрози. Будучи частиною розвідтовариства, NCSC має доступ до розвідувальної інформації про кібершпіонаж та державних хакерів, що підвищує ефективність захисту.

Окрім NCSC, у Великій Британії діють:

– Національний підрозділ кіберзлочинності (NCCU) у складі Національного агентства злочинності – займається розслідуванням серйозних кіберзлочинів, хакерських атак, взаємодіє з Інтерполом, Європолом тощо.

– Оборонна кіберкоманда (Defence Cyber Operations Group) у складі Міноборони, а також новостворені Національні кіберсили (National Cyber Force) – об'єднання фахівців GCHQ та військових для здійснення наступальних кібероперацій проти ворожих цілей.

– Кіберкоординатор при Кабінеті Міністрів – посада для загальної координації політики (в 2021 р. засновано посаду Координатора з питань кібербезпеки). Також при уряді діють ради і комітети, що відповідають за реалізацію стратегії та розподіл фінансування.

Британська модель наголошує на тісній взаємодії з приватним сектором. NCSC активно працює з бізнес-спільнотою, надаючи консультації і платформу для обміну даними. Функціонує програма Cyber Security Information Sharing Partnership (CISP) – це спільнота, де сотні компаній та

урядових установ обмінюються в режимі реального часу технічною інформацією про загрози. Під керівництвом NCSC проводяться галузеві заходи – від закритих брифінгів для топменеджерів критичних підприємств до відкритих конференцій (наприклад, щорічний CYBERUK). Крім того, уряд підтримує створення регіональних центрів кіберстійкості (Regional Cyber Resilience Centres) – локальних консорціумів поліції, університетів та бізнесу для допомоги малому і середньому бізнесу у підвищенні кіберстійкості. Таким чином, існує багаторівнева система, де інформація і досвід циркулюють між державою та приватними партнерами.

Велика Британія вважається однією з передових країн у підготовці кадрів з кібербезпеки. Ще у школах запроваджуються курси із цифрової грамотності та основ кібербезпеки. Під егідою NCSC діє масштабна програма CyberFirst, спрямована на молодь: проводяться кібервікенди та літні табори для підлітків, стипендії для студентів, конкурси серед дівчат CyberFirst Girls тощо. CyberFirst заохочує молодих людей обирати кар'єру у сфері кібербезпеки, пропонуючи підтримку і практику в урядових структурах чи компаніях-партнерах. На рівні університетів у Великій Британії акредитовано кілька центрів передового досвіду (Academic Centres of Excellence in Cyber Security Education), а новостворена Рада з кібербезпеки (UK Cyber Security Council) займається встановленням професійних стандартів і сертифікацією фахівців.

Ізраїль

Ізраїль – одна з перших країн, яка підняла кібербезпеку до рівня національного пріоритету. Ще у 2011 р. рішенням уряду створено Національне кібербюро при канцелярії прем'єр-міністра, яке заклало основи політики. Оформленням підходів став Національний кіберстратегічний напрям 2017 р., зосереджений на розбудові кіберстійкості та наступальних можливостей. На 2022 р. Ізраїль підійшов до необхідності ухвалити єдиний закон щодо кібербезпеки. У червні 2022 р. уряд опублікував проєкт закону щодо кібербезпеки, який мав би надати додаткові повноваження головному органу – Ізраїльському національному кібердиректорату (INCD). Цей законопроєкт все ще обговорюється (станом на 2025 р., остаточно не прийнятий), але він відображає ізраїльську філософію: максимальна координація із приватним сектором і розмежування цивільної та військової кібервідповідальності. Зокрема, у Пояснювальній записці до законопроєкту наголошено на «безпрецедентному типі співпраці» між державою і бізнесом у відсічі кіберзагроз.

Наразі кіберполітика Ізраїлю базується на урядових постановах і наказах: визначено критичні сектори (енергетика, фінанси, транспорт, телеком тощо) та вимоги до їх захисту; діє обов'язкове повідомлення держави про серйозні інциденти. Ізраїль як провідна кібердержава також має доктрину активної кібероборони – це означає, що поряд із захистом своїх мереж, країна здатна на випереджувальні (наступальні) кібероперації проти супротивників. Ця доктрина не прописана в законах, але реалізується через військові структури (наприклад, підрозділ 8200).

Унікальною рисою Ізраїлю є підпорядкування кібербезпеки безпосередньо офісу прем'єр-міністра. Ізраїльський національний кібердиректорат (INCD) – центральний орган, відповідальний за всю національну кіберстратегію і захист цивільної інфраструктури. Він створений у 2018 р. шляхом об'єднання Кібербюро та Національного кіберуправління безпеки. INCD напряму підзвітний прем'єр-міністру і має провідну роль в оцінці національних кіберризиків, плануванні заходів реагування і видачі обов'язкових вказівок іншим відомствам та приватному сектору. За задумом нового закону, INCD отримає ще ширші повноваження, зокрема, право давати нормативні настанови регуляторам фінансів, енергетики, охорони здоров'я та інших галузей щодо кіберзахисту. INCD також оперує двома основними центрами: національний CERT-IL (оперативний центр реагування на інциденти) і центр раннього виявлення атак та обміну інформацією, де агрегуються дані про загрози з держсектора і бізнесу.

Військова і розвідувальна частина кібербезпеки Ізраїлю винесена за рамки INCD. Ізраїльські сили оборони (IDF) мають власні кіберпідрозділи: легендарний підрозділ 8200 відповідає за розвідку і наступальні кібероперації, а управління C4I (командування кіберзахисту) – за оборону військових мереж та IT-систем. Спецслужби Шин-Бет (внутрішня безпека) та Моссад (зовнішня розвідка) також виконують кіберфункції: Шин-Бет опікується захистом критичних об'єктів від кібершпіонажу і тероризму, Моссад – зовнішні наступальні операції. Ці структури співпрацюють з INCD, хоча часом виникає напруга через перетин сфер впливу. Уряд постійно балансує, розділяючи цивільний кібер (INCD) і військовий/розвідувальний кібер (IDF, спецслужби) – так, проєкт закону чітко виключає з повноважень INCD активну протидію хакерам, залишаючи це військовим та розвідникам.

Щодо співпраці з приватним сектором, то ізраїльський підхід часто називають start-up nation у кібербезпеці. Держава активно стимулює співпрацю з бізнесом та наукою в цій галузі. Найвідоміший приклад – кібер-парк CyberSpark в місті Беер-Шева, де поруч розташовані наукові лабораторії Університету Бен-Гуріона, відділення провідних кіберкомпаній і підрозділи INCD. Це створює унікальну екосистему обміну знаннями та швидкого впровадження інновацій. Урядові гранти і програми через ізраїльське Міністерство економіки заохочують створення стартапів у сфері кібербезпеки, багато з яких потім експортують технології по всьому світу (частка Ізраїлю – ~15 % світових інвестицій у кіберіндустрію на 2022 р.). INCD регулярно проводить навчання та діалоги з приватними компаніями. Примітно, що у проєкті закону закладено положення: якщо конкуруючі приватні компанії співпрацюють між собою та з INCD для кіберзахисту, вони отримують імунітет від антимонопольних претензій – настільки держава зацікавлена в повній відкритості інформації про загрози між бізнесами. Великі корпорації зобов'яжуть щорічно звітувати на рівні ради директорів про кіберризики і виконання рекомендацій INCD.

Фундаментом ізраїльського кадрового потенціалу є обов'язкова військова служба. Багато підлітків ще в школі мріють потрапити у престижні технічні підрозділи на кшталт 8200. В армії вони отримують глибоку технічну освіту – від програмування до аналізу кібершпигунства – після чого, відслуживши, часто йдуть у приватний сектор або продовжують службу професійно. Цей безперервний потік талантів створює ефект синергії між військом і високотехнологічним сектором. На цивільному рівні Ізраїль теж активно виховує спеціалістів: діють державні програми підготовки молоді до служби в кіберпідрозділах (наприклад, гуртки Magshimim для школярів). Університети (Тель-Авівський, Техніон, Бен-Гуріона) мають провідні наукові центри з кібербезпеки. Ізраїльські компанії часто співпрацюють з університетами, фінансуючи стипендії та дослідження. Ринок праці дуже активно поглинає випускників – попит на кіберфахівців високий як всередині країни, так і в міжнародних корпораціях, що відкривають R&D-офіси в Ізраїлі.

Нідерланди

Нідерланди як член ЄС формують політику кібербезпеки в руслі європейських директив. У 2018 р. набув чинності Закон «Про безпеку мережевих та інформаційних систем» (Wet Beveiliging Netwerken Informatiesystemen, WBNI) – національний акт, що імплементував директиву NIS. Цей Закон зобов'язує визначені essential services (основні послуги) – енергопостачання, фінансові послуги, постачання води тощо – дотримуватись вимог кібербезпеки і повідомляти про серйозні інциденти, під наглядом державних регуляторів. Також WBNI охопив digital service providers (онлайн-майданчики, хмарні сервіси) відповідно до вимог ЄС. У жовтні 2022 р. уряд затвердив нову Національну стратегію кібербезпеки Нідерландів на 2022–2028 рр., яка ставить за мету «цифрово безпечні Нідерланди». Стратегія підкреслює відповідальність уряду за захист громадян і бізнесу, розвиток публічно-приватного співробітництва та посилення міжнародної співпраці. На базі NIS2 (2022) Нідерланди готують новий закон «Про кібербезпеку» – відповідний законопроєкт

внесено у травні 2024 р., і очікується, що у 2025 р. він набуде чинності, розширивши перелік секторів і вимоги до них.

Головним компетентним органом є Національний центр кібербезпеки (NCSC-NL), що входить до складу Міністерства юстиції і безпеки. NCSC виступає експертним центром та інформаційним вузлом: відстежує кіберзагрози, випускає попередження, консультує організації щодо захисту, а в разі інцидентів – допомагає координувати реагування. Спершу, NCSC було частиною Національного координатора з питань боротьби з тероризмом і безпеки (NCTV), що забезпечувало узгодження з загальною безпековою політикою. Після 2018 р. NCSC отримав статус незалежного підрозділу у структурі Мін'юсту, щоб мати змогу виконувати законодавчі функції нагляду за виконанням WBNI. Проте йому бракувало примусових повноважень – скоріше, центр діяв як координатор і порадник. Тому уряд вирішив розширити та підсилити інституційну спроможність: у 2022 р. анонсовано плани об'єднати NCSC з двома іншими структурами – голландським CERT для цифрових постачальників (CSIRT-DSP) та Цифровим траст-центром (DTC) – в єдине національне кібербезпекове відомство. Цей новий орган, формування якого заплановане до 2026 р., має стати центральною точкою для всіх секторів суспільства (уряду, бізнесу, громадян) з питань кіберзахисту, об'єднуючи експертний центр, команду реагування та інформаційну службу під одним дахом.

Нині ж у Нідерландах паралельно діють:

– NCSC-NL – працює з критично важливими організаціями та урядом, інформацію для інших передає через DTC.

– Digital Trust Center (DTC) при Мінекономіки – орієнтований на малий і середній бізнес поза критичними секторами. DTC надає рекомендації, запроваджує програми підтримки галузевих об'єднань, зокрема гранти на підвищення кіберстійкості для груп підприємств.

– Кіберполіція – підрозділи поліції, які займаються кіберзлочинами (від фінансових шахрайств до зламів).

– Служби розвідки AIVD і MIVD – цивільна та військова розвідки, які теж мають кіберпідрозділи для контррозвідки і кібероперацій проти ворожих державних акторів.

– Міністерства-секторальні регулятори – наприклад, центральний банк для фінансових установ, Міністерство охорони здоров'я для лікарень – які відповідають за контроль кібербезпеки у своїх сферах за вимогами WBNI.

Для стратегічного діалогу в Нідерландах створено Кібербезпекову раду (Cyber Security Council) – впливовий консультативний орган при уряді. До його складу входять 18 осіб: по 7 представників від державного і приватного секторів та 4 – від наукової спільноти. Рада розробляє рекомендації з ключових питань кіберполітики і сприяє тому, щоб голос бізнесу і науки був почутий урядом. Її рекомендації часто слугують основою для нових ініціатив.

Нідерланди характеризуються культурою довіри і партнерства між державою та підприємцями. NCSC та DTC постійно проводять спільні заходи (тренінги, семінари). Наприклад, DTC фінансувало проєкти, де кілька МСП об'єднувалися для колективного підвищення безпеки (обмін фахівцем з кібербезпеки або спільна система моніторингу). У фінансовому секторі центральний банк і регулятори запровадили програми TIBER-NL – це спільне тестування банків на стійкість шляхом етичних хакерських атак, щоб виявити слабкі місця. У цілому, приватні компанії в Нідерландах охоче обмінюються інформацією про інциденти через платформи, підтримувані NCSC. Нідерланди також відомі міжнародними ініціативами: саме в Гаазі знаходиться Європейський центр кіберзлочинності Європолу, Організація по забороні хімічної зброї (яка теж під кіберзагрозами – голландці допомагали викривати кібернапади на неї у 2018 р.). Тобто співпраця виходить за межі країни – Нідерланди позиціонують себе як хаб міжнародного діалогу з кібербезпеки.

Кадрове питання вирішується через поєднання освіти і перекваліфікації. У Нідерландах працюють кілька профільних освітніх програм, наприклад, магістерська

програма Cyber Security Academy в Гаазі (спільний проєкт кількох університетів). Держава фінансує дослідження у сфері кібербезпеки – університети отримують гранти на інновації. Також є увага до кадрів у державному секторі: розроблені програми навчання для державних службовців (як діяти при фішингових атаках, менеджмент інформаційної безпеки тощо). Варто відзначити, що Нідерланди входять до консорціуму європейських кіберполігонів і регулярно беруть участь у спільних навчаннях (наприклад, кібернавчання НАТО Locked Shields). Це дає голландським фахівцям можливість підвищувати кваліфікацію в реалістичних умовах.

Німеччина

Німеччина послідовно вибудувала правове поле кібербезпеки, спираючись на свою федеративну систему та вимоги ЄС. Ще у 2015 р. було ухвалено Закон «Про ІТ-безпеку» (IT-Sicherheitsgesetz), який зобов'язав операторів критичної інфраструктури повідомляти про кібератаки і дотримуватись мінімальних стандартів безпеки. У 2021 р. цей Закон оновили (так званий IT-Sicherheitsgesetz 2.0), суттєво розширивши список критичних секторів та надавши додаткові повноваження Федеральному відомству з інформаційної безпеки (BSI). Наприклад, введено вимогу обов'язкової сертифікації безпеки для важливого ІТ-обладнання і право BSI перевіряти продукти на наявність бекдорів. Також німецький уряд імплементував директиву NIS через поправки до Закону щодо BSI і секторного законодавства. Нові вимоги NIS2, ймовірно, набудуть чинності через чергові зміни у 2024–2025 рр., ще більше піднімаючи планку безпеки для бізнесу. Паралельно діють норми захисту персональних даних (GDPR та німецький Федеральний закон щодо захисту даних), які теж впливають на кібербезпеку. Національна Стратегія кібербезпеки Німеччини була затверджена у 2021 р. – вона визначає пріоритети, такі як захист державних мереж, посилення ролі BSI, розвиток криптографічних рішень і створення європейської цифрової автономії.

Центральною ланкою є Федеральне відомство з безпеки інформаційних технологій (BSI) – авторитетний орган, заснований ще в 1991 р. BSI – це національний центр кібербезпеки Німеччини, відповідальний за захист критичної інфраструктури, встановлення стандартів безпеки та реагування на кіберзагрози. BSI підпорядковується Міністерству внутрішніх справ і має широкий мандат: від випуску рекомендацій та сертифікації ІТ-продуктів до аналізу кіберінцидентів і координації захисту урядових мереж. При BSI діє національна команда реагування CERT-Bund, що обслуговує держустанови, а також Allianz für Cyber-Sicherheit (ACS) – Альянс кібербезпеки, створений BSI спільно з галузевою асоціацією Bitkom для налагодження обміну інформацією з бізнесом. Альянс об'єднує тисячі компаній та організацій, які отримують від BSI сповіщення про загрози, навчальні матеріали і можуть обмінюватися досвідом між собою.

Іншими важливими бійцями кіберфронту є:

– Федеральне відомство із захисту конституції (BfV) – контррозвідка, моніторить кібероперації іноземних спецслужб проти Німеччини, попереджає критичні компанії про шпигунську активність.

– Федеральна розвідувальна служба (BND) – здійснює зовнішню кіберрозвідку та наступальні операції за кордоном (зокрема, слідкує за діяльністю хакерських груп поза межами країни).

– Кібер-командування Бундесверу (Kommando Cyberund Informationsraum), засноване у 2017 р., – інтегрує військові можливості захисту й атаки в кіберпросторі, захищає військові мережі та виконує завдання у зонах операцій.

– На рівні земель (регіонів) кожна федеральна земля має свої підрозділи кіберзахисту в поліції та органах влади, що координуються з BSI.

– Особливістю німецької системи є федерально-земельна співпраця: після кібернападу на м. Люксембург або шпиталь у Дюссельдорфі, локальні ІТ-служби діють перші, але BSI та федеральна поліція можуть підключатися для підтримки. У 2022 р. Німеччина почала створювати єдиний центр кіберзахисту із представників федерації і земель, щоб підвищити узгодженість дій.

BSI історично будує партнерство з бізнесом через добровільні ініціативи. Альянс кібербезпеки (ACS), започаткований у 2012 р., пропонує членам (понад 5000 організацій) широкий спектр послуг: тренінги, спільні вправи, розсилку сповіщень про уразливості, платформу для діалогу експертів. BSI також має програму IT-Grundschutz – набір базових стандартів і рекомендацій з кібербезпеки, який оновлюється щорічно і яким можуть керуватися компанії будь-якого розміру. Виконання цих стандартів є добровільним, але фактично стало «де-факто» нормою: багато німецьких підприємств сертифікуються за ISO 27001 на базі IT-Grundschutz, демонструючи відповідність перед регуляторами і партнерами.

При BSI діє «Діалог з кібербезпеки» – форум, де представники різних секторів регулярно зустрічаються з експертами BSI для обговорення нових загроз і спільного вироблення підходів. Цей діалог допомагає BSI враховувати інтереси бізнесу при підготовці регуляцій. Законодавчо у 2021 р. запроваджено цікаву норму: компанії, що постачають критичне обладнання (наприклад, для телекомів), повинні давати гарантії прозорості і безпеки; невиконання може призвести до їх недопущення на ринок (так було фактично створено механізм обмеження постачальників типу Huawei в 5G). Таким чином, співпраця в Німеччині поєднує добровільність і регуляторний тиск: більшість компаній добровільно дотримуються рекомендацій BSI, розуміючи, що інакше держава може зробити вимоги обов'язковими.

Університети Німеччини пропонують численні програми з кібербезпеки – як технічні, так і управлінські. Відомі центри – Бохумський університет (криптографія), Технічний університет Мюнхена тощо. BSI співпрацює з вишами, надаючи підтримку програмам підготовки і стажування студентів. Для працівників компаній BSI і промислові асоціації організовують курси підвищення кваліфікації. Крім того, з 2019 р. за ініціативи уряду та промисловості створено Агентство з інновацій у кібербезпеці (Cyberagentur) – воно фінансує проривні наукові проєкти, що часто передбачають залучення аспірантів, молодих науковців. Німеччина також реалізує програми Digitalpakt Schule – інтеграція IT та кібернавичок у школи, щоб з раннього віку виховувати нове покоління IT-фахівців. Серед неформальних ініціатив – щорічні змагання BSI Cyber Cup для молоді, хакатони за підтримки бізнесу тощо.

При цьому різні країни у своїх моделях кібербезпеки роблять наголоси на різних моментах. США та Велика Британія роблять акцент на партнерстві з бізнесом та розвитку кадрів; Ізраїль – на військово-технічній синергії та інноваціях; Китай – на державному контролі і масштабності; Нідерланди – на громадській співпраці та довірі; Німеччина – на стандартах і федеративній координації. Україна, будуючи свою систему, враховує цей досвід, адаптуючи його до умов війни та власних ресурсів.

Китай

Китай підходить до кібербезпеки з позиції національного суверенітету та контролю над інформаційним простором. У 2017 р. набув чинності всеосяжний Закон КНР «Про кібербезпеку», який встановив вимоги до мережевих операторів, критичної інформаційної інфраструктури (КІІ) та ввів поняття «суверенітету кіберпростору». Цей Закон зобов'язує операторів КІІ (банки, транспорт, енергетика, телеком та ін.) забезпечувати безпеку мереж на рівні державних стандартів, проводити аудит і зберігати дані в межах Китаю. У 2021 р. правова база доповнилася Законом «Про безпеку даних» та Законом «Про захист особистої інформації», які регулюють поводження з даними та конфіденційність. Для конкретизації положень Закону «Про кібербезпеку», Державна рада КНР видала Положення про охорону критичної інформаційної інфраструктури (2021) – вони визначили, які саме об'єкти належать до КІІ, і які органи за них відповідають. Згідно з цими правилами, Міністерство громадської безпеки (MPS) очолює захист КІІ на національному рівні, галузеві регулятори встановлюють вимоги у своїх секторах, а Адміністрація кіберпростору Китаю (CAC) координує загальну політику та обмін інформацією. Фактично, Китай сформував потужний режим кіберрегулювання:

ліцензування IT-продуктів, сертифікація обладнання для критичних мереж, цензура трафіку і контенту (т.зв. «Великий китайський фаєрвол»), контроль транскордонної передачі даних тощо.

На самому верху китайської моделі інституційної ієрархії стоїть Центральна комісія з питань кібербезпеки та інформатизації, очолювана особисто головою КНР. Виконавчим органом Комісії є згадана CAC (Адміністрація кіберпростору Китаю), яка розробляє стратегії, політики та цензурує інтернет-контент. Окремо Міністерство громадської безпеки (MPS) через свій Бюро кібербезпеки опікується саме технічним захистом мереж та боротьбою з кіберзлочинністю – MPS, по суті, китайська «кіберполіція». Міністерство держбезпеки (розвідка) та підрозділи Народно-визвольної армії займаються наступальними кіберопераціями і шпигунством. Важливу роль грає Міністерство промисловості та інформтехнологій (MIIT) – воно встановлює стандарти для телекомів та IT-індустрії, відповідає за реалізацію технічних програм на кшталт впровадження мереж 5G з урахуванням безпеки. Таким чином функції розподілені: CAC – політика і цензура, MPS – захист критичних систем і боротьба з кіберзлочинами, MIIT – технічні стандарти і розвиток інфраструктури, військові/спецслужби – наступальні операції. Координація між ними здійснюється через міжвідомчі механізми, хоча в минулому спостерігалася конкуренція відомств. Зокрема, створення CAC у 2014 р. було покликане подолати розбіжності між силовиками щодо підходів до кібербезпеки.

На практиці Китай будує багаторівневу систему кіберзахисту: діє стара система багаторівневого захисту інформації (MLPS) під керівництвом MPS, тепер оновлена до версії 2.0, яка зобов'язує організації класифікувати свої інформаційні системи за рівнем важливості і впроваджувати відповідні міри безпеки. Паралельно – новий режим захисту КІІ, де ключовим є аудит і моніторинг. Наприклад, після інциденту з компанією Didi (яка вийшла на IPO за кордон), влада використала закони щодо кібербезпеки, щоб провести розслідування і визнати Didi оператором КІІ, обмеживши її діяльність. Це показовий крок, що підкреслює принцип: критичні дані і сервіси мають бути під контролем держави.

У Китаї співпраця системи кіберзахисту з приватним сектором часто набуває форми примусової відповідності вимогам. Великі технологічні компанії (Baidu, Alibaba, Tencent тощо) тісно співпрацюють з урядом, виконуючи вимоги щодо цензури і безпеки, а також ділячись даними. Китайські закони, зокрема, Закон «Про національну розвідку» (2017), зобов'язують компанії сприяти державним органам у питаннях національної безпеки. Водночас держава інвестує у розвиток вітчизняної кіберіндустрії: існують державні програми підтримки виробників засобів кіберзахисту, криптографії, антивірусів тощо, щоб зменшити залежність від іноземних технологій. Проводяться масштабні національні кібервиставки (наприклад, China Cybersecurity Week) для популяризації рішень. Таким чином, модель КНР – це тісне злиття держави і бізнесу в питанні безпеки: приватний сектор виконує встановлені державою «правила гри» та отримує величезний внутрішній ринок, що стимулює інновації.

Китай стикається з колосальними потребами в кіберфахівцях для своєї цифрової економіки. Тому в країні започатковано масштабне розгортання освітніх програм. Станом на 2024 р., 626 університетів Китаю відкрили спеціальності, пов'язані з кібербезпекою – вражаюча цифра, яка демонструє прискорений розвиток кіберосвіти. У провідних технічних вузах (Університет Цінхуа, Харбінський технологічний інститут та ін.) створено факультети кібербезпеки. Під патронатом уряду проводяться олімпіади, змагання з кібербезпеки серед студентів (наприклад, China Cybersecurity Competition). Військові академії також випускають тисячі кіберофіцерів для армії. За оцінками аналітиків, незважаючи на ці зусилля, до 2027 р. Китаю може бракувати ще понад 3 млн фахівців у сфері мережевої безпеки – настільки швидко ростуть цифрові загрози і потреба в захисті. Щоб закрити цю прогалину, влада стимулює курси перекваліфікації

(наприклад, для ІТ-фахівців суміжних галузей) та створює національні центри підготовки. Один із прикладів – відкриття в 2020 р. Національного центру кібербезпеки в Ухані, здатного навчати до 70 тис. людей на рік. Китай робить ставку на масовість: підвищення обізнаності населення (програми кібергігієни для громадян), навчання для держслужбовців, інтеграція тем кібербезпеки у шкільну програму.

Тож Україна стоїть на порозі якісного стрибка у сфері кібербезпеки: нове законодавство, інституційні зміни, міжнародна допомога та власний гіркий досвід кібервійн з Російською Федерацією формують сучасну національну кіберстратегію. Вивчення найкращих практик США, Британії, Ізраїлю, Китаю, Нідерландів, Німеччини дозволяє адаптувати перевірені рішення – від побудови національного центру реагування до програм розвитку кадрів ***(Статтю підготовлено з використанням інформації таких джерел: Офіційний вебпортал парламенту України (https://www.rada.gov.ua/news/razom/260570.html; https://itd.rada.gov.ua/billInfo/Bills/Card/44275); Державна служба спеціального зв'язку та захисту інформації України (https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv; https://cip.gov.ua/ua/news/nacionalna-sistema-kiberbezpeki-funkcionuvatime-efektivnishe); Рада національної безпеки і оборони України (https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf); вебсайт Hromadske (https://hromadske.ua/polityka/242216-v-ukrayini-ziavliatsia-systemy-reahuvannia-na-kiberataky-rada-skhvalyla-zakonoproyekt); вебсайт Dev Україна (https://dev.ua/news/nardep-fediienko-proponuie-viddaty-pytannia-kiberzakhystu-vid-derzhavy-na-autsors-zapiat-rokiv-u-parlamenti-tak-i-ne-zrozumilyshcho-take-kiberbezpeka; https://dev.ua/news/za-8-rokiv-ukrainskyi-rynok-kiberbezpeky-zbilshyvsia-na-ponad-100-mln-iaka-chastka-ukrainy-na-svitovomu-rynku-1736260316; https://dev.ua/news/tam-bulo-nedostatno-liudei-nalezhnoi-kvalifikatsii-z-kiberzakhystu-a-sama-systema-finansuvalasia-za-zalyshkovym-pryntsypom-ekspert-korsun-pro-prychyny-i-naslidky-kiberataky-na-reiestry-1737447007; https://dev.ua/news/monopoliia-postachalnykiv-posluh-pidkup-abo-fishynh-iaki-imovirni-prychyny-kiberataky-na-derzhreiestry-1734944772); вебсайт ITTA INFO (https://itta.info/derzhavna-polityka-kiberbezpeky-ukraina-ta-mizhnarodnyy-dosvid/); вебсайт «Правова база української кібербезпеки: загальний огляд і аналіз» (https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf); Науковий вісник Ужгородського Національного Університету (https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/09/14-2.pdf); Інтернет-журнал «Кібербез» (https://cybersec.net.ua/normatyvni-dokumenty/793-ukraina-vprovadzhuie-naikrashchi-svitovi-praktyky-u-sferi-kiberbezpeky-ta-vprovadzhuie-normy-nist-cybersecurity-framework-20.html; https://cybersec.net.ua/normatyvni-dokumenty/820-zatverdzheno-plan-zakhodiv-na-2025-rik-z-realizatsii-stratehii-kiberbezpeky.html; https://cybersec.net.ua/normatyvni-dokumenty/774-poiasniuvalna-zapyska-do-proiektu-zakonu-ukrainy-pro-kibersyly-zbroinykh-syl-ukrainy.html; https://cybersec.net.ua/normatyvni-dokumenty/775-zatverdzheno-novi-rekomendatsii-ta-formu-planu-zakhystu-vid-kiberzahroz-dlia-obiektiv-krytychnoi-infrastruktury.html); вебсайт «Укрінформ» (https://www.ukrinform.ua/rubric-society/3950535-minust-zvilniv-kerivnika-dp-nacionalni-informacijni-sistemi-pisla-kiberataki-na-derzreestri.html); Центр прав людини ZMINA (https://zmina.info/news/rada-progolosuvala-za-stvorennya-systemy-reaguvannya-na-kiberataky-hochut-pryhovuvaty-dani-pro-inczydenty/); вебсайт «Комерсант український» (https://www.komersant.info/v-ukraini-z-iavliatsia-systemy-reahuvannia-na-kiberataky-rada-pryyniala-zakon/)).***

О. Кривецький, мол. наук. співроб., НЮБ НБУВ

Повноваження Нацгвардії: розширення чи уніфікація

На розгляді Верховної Ради України перебуває законопроєкт № 10311 «Про внесення змін до Закону України "Про Національну гвардію України" щодо вдосконалення правових засад застосування заходів примусу військовослужбовцями Національної гвардії України». У разі його ухвалення нацгвардійці отримають право застосовувати проти цивільного населення під час масових заходів протесту вогнепальну зброю, гумові кийки, електрошокери, сльозогінний газ та безпілотники. Авторами документа зазначено, що законопроєкт спрямовано на вдосконалення правового регулювання питань, що пов'язані із застосуванням військовослужбовцями НГУ заходів примусу, зокрема, фізичного впливу, спеціальних засобів, зброї та бойової техніки з метою якісного виконання завдань, покладених на НГУ.

Законопроєкт передбачає низку нововведень, а саме:

– застосування зброї дозволяється після попередження через гучномовці або електронні табло;

– дозволяється застосування засобів обмеження рухливості, такі як наручники, сітки для зв'язування, а також спеціальні фарби для маркування правопорушників;

– військовослужбовці отримують право застосовувати примус для затримання осіб, які намагаються уникнути перевірки на блокпостах;

– забороняється застосування примусових заходів щодо вагітних жінок, літніх людей, дітей та осіб з інвалідністю (однак, ця заборона знімається у випадках групового чи збройного нападу);

– НГУ дозволяється використовувати дрони для спостереження, маркування правопорушників та інших оперативних завдань.

Схвалення цього законопроєкту у березні поточного року профільним Комітетом ВРУ викликало значний суспільний резонанс.

Так, у Центрі протидії корупції (ЦПК) вважають ці повноваження надмірними і такими, що можуть становити небезпеку для здоров'я людей і загрозу життю цивільних громадян. Наголошується також, що положення законопроєкту не мають нічого спільного з підвищенням ефективності захисту країни і несуть грубі порушення конституційних прав українських громадян. «Законопроєкт значно розширює повноваження Національної гвардії України (НГУ), надає практично необмежені права для використання вогнепальної зброї, сльозогінного газу, електрошокерів, безпілотників та інших засобів впливу, й у разі його ухвалення влада фактично отримає повну індульгенцію на жорстке і необмежене придушення будь-яких громадянських протестів та масових заворушень», – зазначила заступник виконавчого директора ЦПК, адвокат О. Щербань.

Голова правління «Центру протидії корупції» В. Шабунін також зазначає, що зміни, запропоновані у законопроєкті № 10311, здатні призвести до порушення основоположних прав і свобод громадян, а нацгвардія може отримати право використовувати вогнепальну зброю без належного попередження, маркувати учасників протестів та застосувати безпілотні апарати для спостереження і електрошокери для ураження порушників без нагальної потреби. «Щодо застосування безпілотників, то в законопроєкті взагалі немає роз'яснень, яким чином їх будуть застосовувати, і які будуть обмеження на їх застосування», – каже він.

Міністерство внутрішніх справ України надало роз'яснення положень цього документа, зазначивши, що насправді в цьому законопроєкті повноваження НГУ не розширять, а «впорядкують» з метою підвищення ефективності НГУ у виконанні завдань із забезпечення громадського порядку та захисту держави в умовах війни. У Департаменті комунікацій МВС заспокоюють суспільство та запевняють, що

жодних негативних змін не відбудеться, адже нацгвардійці використовували засоби примусу і раніше. Так, у переліку спеціальних засобів, що застосовуються військовослужбовцями Національної гвардії України під час виконання службових завдань, затвердженому ще Постановою КМУ від 20.12.2017 р. № 1024, визначено, що до них належать в тому числі: гумові та пластикові кийки, електрошокові пристрої контактної та контактно-дистанційної дії, кайданки, сітки для зв'язування, засоби споряджені речовинами сльозогінної та дратівливої дії та ін.

Разом з тим, у Правилах застосування спеціальних засобів військовослужбовцями Національної гвардії під час виконання службових завдань, затверджених цією Постановою, визначено, що в разі залучення військовослужбовців Національної гвардії до виконання завдань з охорони громадського порядку застосування спеціальних засобів здійснюється відповідно до ст. 45 Закону України «Про Національну поліцію», яка фактично повністю продубльована авторами законопроєкту в доповненні до існуючої ст. 17 Закону України «Про Національну гвардію України». Отже, НГУ дійсно вже наділено повноваженнями застосовувати спеціальні засоби, однак, станом на зараз військовослужбовець НГУ має використовувати норми багатьох нормативно-правових документів одночасно та користуватися законами, які регулюють діяльність інших структур, зокрема Національної поліції України (НПУ). Крім того, юристи МВС зазначають, що в законопроєкті у ст. 18 також продубльовано ст. 46 ЗУ «Про Національну поліцію» щодо застосування вогнепальної зброї. За їх словами, НГУ мала і має право застосовувати вогнепальну зброю, тому резонанс щодо надання НГУ в законопроєкті такого права – безпідставний.

При цьому не можна стверджувати, що надані роз'яснення задовольнили критиків ініціативи. Так, нардеп від партії «Голос» Я. Железняк звертає увагу на виключення авторами законопроєкту пунктів щодо певних випадків заборони застосування вогнепальної зброї. Саме ці положення з невідомих причин були виключені авторами законопроєкту з чинного ЗУ «Про Національну гвардію України» та не продубльовано із ЗУ «Про Національну поліцію України», хоча останній містить пункт: «…заборонено застосовувати вогнепальну зброю в місцях, де може бути завдано шкоди іншим особам, а також у вогненебезпечних та вибухонебезпечних місцях, крім випадків необхідності відбиття нападу або за крайньої необхідності». Як наголошує депутат, НГУ могла і може використовувати вогнепальну зброю, проте, в чинному Законі це можливо «у випадку виключної необхідності», тоді як законопроєкт лише визначає, що «застосування зброї є найбільш суворим заходом примусу».

В умовах сучасних викликів, що стоять перед Україною, зокрема в контексті воєнного стану, надзвичайно важливо мати чітко визначені та законодавчо врегульовані повноваження правоохоронних органів. А Національна гвардія України – це складова системи МВС, структура, що, окрім виконання завдань на лінії фронту, має правоохоронні завдання. Військовослужбовці НГУ несуть службу на блокпостах, виконують правоохоронні функції на деокупованих та прифронтових територіях, а також залучаються до контрдиверсійних заходів і боротьби з ДРГ. Під час виконання своїх зобов'язань та повноважень вони керуються різними законодавчими актами, серед яких, зокрема Закон України «Про Національну поліцію». Тож авторами законопроєкту дійсно зроблено спробу уніфікувати норми багатьох нормативно-правових актів в одному законі, який передбачає розширення повноважень НГУ і регулює її діяльність. Проте Міністерство внутрішніх справ України не надає чіткого пояснення, яким чином боротьба з масовими акціями протесту пов'язана з протидією диверсійно-розвідувальним групам (ДРГ), що було офіційним обґрунтуванням законопроєкту. Тому законопроєкт наразі знято з розгляду Верховної Ради України і надіслано на доопрацювання ***(Статтю підготовлено з використанням інформації таких джерел: Офіційний вебпортал парламенту України (https://www.rada.gov.ua/news/news_kom/260269.html/); вебсайт New Voice (https://nv.ua/ukr/***

ukraine/events/v-mvs-poyasnili-chi-mozhe-rada-rozshiriti-povnovazhennya-nacgvardiji-50499927.html/); вебсайт Lexology https://www.lexology.com/library/detail.aspx?g=2490fa14-b6c0-4782-9e49-09dd162695ee/); вебсайт «РБК-Україна» (https://www.rbc.ua/rus/news/natsgvardiyi-poyasnili-zakonoproekt-shchodo-1742582369.html/)).

ЩОДЕННИК БЛОГЕРА *

Блог на сайті «Lb.ua»

Про автора: Кирило Міненко, керівник Центрального міжрегіонального управління Міністерства юстиції (м. Київ)

Право на працю: що необхідно знати про документи та обов'язки роботодавця перед першим робочим днем

Працевлаштування – важливий етап у житті кожної людини. Від правильності оформлення трудових відносин залежать не лише умови роботи, а й правовий захист працівника. Законодавство України передбачає чіткі правила, яких мають дотримуватися як працівники, так і роботодавці ще до моменту початку виконання трудових обов'язків. Звертаю увагу на базові норми, що регулюють порядок призначення на посади, зокрема й у сфері державної служби.

Право на працю закріплене у статті 43 Конституції України. Воно передбачає можливість кожного громадянина на вільний вибір або згоду на працю, справедливу оплату, безпечні та належні умови праці, а також захист трудових прав. Щоб це право було гарантовано на практиці, держава встановила низку обов'язкових норм, які регулюють укладення трудових договорів. Базовими серед них є статті 24 та 29 Кодексу законів про працю України, що забезпечують законне та прозоре оформлення трудових відносин для всіх категорій працівників, у тому числі державних службовців, доповнюючи положення спеціальних законів, зокрема Закону України «Про державну службу».

Так, стаття 24 КЗпП визначає перелік документів, які працівник повинен надати при укладенні трудового договору. Серед них: паспорт або інший документ, що посвідчує особу, трудова книжка (за наявності) або відомості про трудову діяльність з реєстру застрахованих осіб, документи про освіту, кваліфікацію чи професійну підготовку, медичні документи у випадках, передбачених законодавством, військово-облікові документи для військовозобов'язаних, а також інші документи, якщо їх подання передбачене нормативно-правовими актами. Водночас особи, які працевлаштовуються вперше, мають право вимагати оформлення трудової книжки.

Відповідно до статті 29 КЗпП, до початку роботи роботодавець зобов'язаний ознайомити працівника з основними умовами трудових відносин. Працівнику має бути повідомлено про місце роботи, трудову функцію, дату початку виконання обов'язків, умови праці, режим роботи, тривалість робочого часу та відпочинку. Йому необхідно роз'яснити права та обов'язки, правила внутрішнього трудового розпорядку, а також повідомити про наявність небезпечних чи шкідливих виробничих факторів на робочому місці та передбачені для таких випадків пільги та компенсації. Обов'язковим є ознайомлення працівника з положеннями колективного договору, якщо такий укладено на підприємстві, та проведення інструктажу з охорони праці. Крім того, працівнику мають надати інформацію про тривалість щорічної відпустки, порядок і строки попередження у разі припинення трудового договору, а також умови та розмір оплати праці. Вся ця інформація надається працівнику під підпис, що є необхідною умовою належного інформування та правового захисту.

* Збережено стиль і граматику оригіналу

Дотримання вимог статей 24 та 29 КЗпП – загальна та обов'язкова умова для законного призначення працівника на будь-яку посаду. Це забезпечує його трудові права з першого робочого дня, надає можливість працівнику своєчасно отримати необхідну інформацію про свої обов'язки та гарантії, а роботодавцю – належним чином організувати робочий процес та виконати свої обов'язки відповідно до закону. Правильно оформлені трудові відносини – це не лише формальність, а й важливий правовий інструмент, що гарантує стабільність роботи, забезпечує прозорість у взаєминах між працівником і роботодавцем та створює умови для захисту прав та інтересів обох сторін. Саме тому варто приділяти належну увагу оформленню документів та дотриманню процедур, визначених трудовим законодавством України.

Щодо додаткових новації у сфері трудових відносин. 02 травня 2025 року набув чинності Закон України № 4339-IX від 27.03.2025 «Про внесення змін до Кодексу законів про працю України щодо удосконалення правового регулювання окремих питань надомної та дистанційної роботи», відповідно до якого доповнено ст. 60-1 та 60-2 Кодексу законів про працю України такого змісту:

За погодженням із роботодавцем працівник може працювати на умовах надомної роботи у разі навчання його дитини віком до 14 років у закладі загальної середньої освіти за дистанційною формою здобуття освіти відповідно до наказу (розпорядження) керівника такого закладу освіти на період такого навчання.

За погодженням із роботодавцем працівник може працювати на умовах дистанційної роботи у разі навчання його дитини віком до 14 років у закладі загальної середньої освіти за дистанційною формою здобуття освіти відповідно до наказу (розпорядження) керівника такого закладу освіти на період такого навчання.

І пам'ятайте: завдання кожного – не тільки знати закон, а й дотримуватися його в повсякденному житті. Бо право – це не про папери, а про людей. Про їхні можливості, безпеку і впевненість. Тож закликаю роботодавців та працівників бути уважними до деталей, дбати про належне оформлення трудових відносин і пам'ятати: права працювати гідно заслуговує кожен ***(https://lb.ua/blog/kyrylo_minenko/677578_pravo_pratsyu_shcho_neobhidno_znati_pro.html). – 2025. – 21.05).***

***

Блог на сайті «Lb.ua»

Про автора: Дмитро Лубінець, уповноважений Верховної Ради України з прав людини

Чому тема захисту персональних даних є важливою на шляху до вступу в ЄС?

У процесі наближення України до Європейського Союзу захист персональних даних є важливою складовою реформ, спрямованих на забезпечення відповідності європейським стандартам у сфері верховенства права. Одним із головних завдань у цьому напрямі є гармонізація національного законодавства з положеннями Загального регламенту про захист даних (GDPR).

Зазначу, що оновлення законодавства про захист персональних даних та створення незалежного наглядового органу з розширеними повноваженнями є ключовим кроком на шляху до вступу України в Європейський Союз.

Яка роль Офісу Омбудсмана у впровадженні реформ у захисті персональних даних?

Я, як Уповноважений Верховної Ради України з прав людини, беру активну участь у процесах реформування відповідної сфери в контексті євроінтеграції. Окрім того, Офіс Омбудсмана постійно залучається до міжвідомчої взаємодії, робочих зустрічей, а також до підготовки стратегічних документів, спрямованих на адаптацію національного законодавства до права Європейського Союзу.

Так, наш Офіс взяв участь у розробці Плану заходів з виконання рекомендацій Європейської Комісії, представлених у Звіті про прогрес України в межах Пакета розширення Європейського Союзу 2024 року, затвердженого

Кабінетом Міністрів України. План, зокрема, передбачає:

проведення інформаційної кампанії щодо необхідності прийняття Закону України «Про захист персональних даних» у новій редакції, та Закону України «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації»;

проведення просвітницької кампанії щодо оновленого законодавства про захист персональних даних для осіб, відповідальних за обробку персональних даних.

Зазначу, що Офіс Омбудсмана проводить масштабну інформаційну кампанію, спрямовану на роз'яснення ключових положень чинного законодавства, а також очікуваних змін, пов'язаних з імплементацією положень GDPR.

Наголошу, що кампанія має на меті не лише підвищити рівень обізнаності громадян, бізнесу та органів державної влади, а й сприяти формуванню в Україні культури дбайливого та свідомого ставлення до персональних даних в цифрову епоху. До реалізації кампанії залучені фахівці Офісу Омбудсмана, а також експерти, представники державних органів і громадянського суспільства, та міжнародні партнери.

Ключовими елементами кампанії є:

регулярні тематичні публікації на моїх офіційних сторінках в соціальних мережах;

проведення освітніх заходів, конференцій та круглих столів для державних службовців, представників бізнесу, громадського сектору;

організація тренінгів та навчальних семінарів, що роз'яснюють нові правові механізми захисту даних, які з'являться після ухвалення законодавчих змін.

Чому інформаційна кампанія із захисту персональних даних важлива для євроінтеграції?

На мою думку, ця інформаційна ініціатива є важливою частиною глобального процесу реформ у сфері прав людини, що має забезпечити Україні позитивну оцінку з боку Європейської Комісії у сфері верховенства права та сприяти подальшому просуванню на шляху до членства в Європейському Союзі ***(https://lb.ua/blog/dmytro_lubinets/677944_chomu_tema_zahistu_personalnih_danih.html). – 2025. – 23.05).***

***

Блог на сайті «Цензор.НЕТ»

Про автора: Ярослав Романчук, науковий керівник Українського інституту економічного лідерства

Надра в обмін на розвиток

Подія, яка претендує на статус головної для країни не лише цього року, а й за всю історію американсько-українських відносин – угоду щодо рідкісноземельних металів між урядом США та України після довгих перемовин було підписано 30 квітня 2025 року та ратифіковано.

Угода під назвою «CPM-US-UA» – це точно не типова комерційна угода – у ній занадто багато «води», нехарактерної для такого роду договорів. Разом з тим, цей договір не є типовим для стандартних міжнародних договорів про дружбу і партнерство між країнами, тому що в його основі – цілком певні товари. Цю угоду не можна вважати правовим базисом спільної системи безпеки: там немає того, що притаманне договорам про безпеку.

Угода CPM-US-UA – це правовий, інституційний гібрид між двома країнами, кожна з яких бачить у ній те, що хоче. Вона поєднує різні уявлення, вимоги та проєкції майбутнього урядів двох країн і може стати основою стратегічного партнерства між США та Україною в найрізноманітніших сферах: від енергетики та видобувної промисловості до безпеки. Але цей потенціал сам себе не реалізує, необхідно виконати величезну роботу насамперед українській стороні.

Для американської сторони дана угода – це документальне підтвердження попиту на рідкоземельні метали, на декитаїзацію ланцюжків пропозиції цих критично важливих компонентів сучасного виробництва різних видів товарів. Якщо в Україні є те, що потрібно США для своїх стратегічних цілей, для зміцнення безпеки, для створення повного циклу виробництва сучасних товарів у рамках

країн Вісі Добра і чесноти Свободи, тоді за цю нішу потрібно чіплятися обома руками.

Та чи є в Америки те, що потрібно Україні?

Стратегічне партнерство двох країн було б подарунком долі для нашої країни, але його потрібно заслужити. Для цього необхідно стати своїм для американських політичних, економічних еліт. Серед обох партій США, Україна має сприйматися, як своя прозахідна, вільна, тобто одного поля ягода. Поки що цього немає, бо останні 30 років українські політичні, економічні, номенклатурно-силові еліти займалися не вибудовуванням стратегічного партнерства з потужними, ресурсними, авторитетними країнами, структурами та організаціями, а радше вирішували свої шкурні, вузьковідомчі питання. Вони не були готові до повноцінного партнерства, до надання доступу іноземному капіталу до багатих ресурсів України ***(https://censor.net/ua/blogs/3553442/nadra-v-obm-n-na-rozvitok). – 2025. – 21.05).***

***

Блог на сайті «Українська правда»

Про автора: Гюндуз Мамедов, кандидат юридичних наук, заступник Генпрокурора України у 2019-2022 рр.

Право знати: понад 400 000 зниклих безвісти

Станом на квітень 2025 року українські родини подали щонайменше 400 000 звернень щодо зниклих безвісти осіб. Такі дані наводить Міжнародний Комітет Червоного Хреста. Проте навіть ця цифра не відображає повної картини. У статистику потрапляють як цивільні особи, так і військовослужбовці, щодо яких немає підтвердження загибелі або полону. Часто за фактом «зникнення» стоїть загибель у зоні бойових дій або перебування в полоні, яке російська сторона відмовляється визнавати. Водночас значна частина зниклих, особливо на тимчасово окупованих територіях, залишається поза обліком – через відсутність доступу, бойову обстановку, блокування інформації з боку РФ і цілеспрямоване приховування фактів.

Міжнародне гуманітарне право, зокрема Женевські конвенції 1949 року та Додатковий протокол I, покладає на сторони збройного конфлікту обов'язок встановлювати долю зниклих, вести облік полонених, передавати цю інформацію МКЧХ, гідно поводитися з тілами загиблих і забезпечувати повернення тіл родинам. Це не просто гуманітарна норма – це юридичне зобов'язання, що захищає не лише живих, а й померлих. Право на гідне ставлення не припиняється після смерті.

На практиці Російська Федерація системно порушує ці вимоги. Часто не підтверджуються факти полону, навіть якщо є свідки або фото– та відеодокази. Немає доступу до місць тримання, ігноруються запити МКЧХ, не ведеться офіційна реєстрація. Особливо складною залишається ситуація з тими, хто загинув у боях: евакуація тіл у зоні активних зіткнень нерідко неможлива через щільний вогонь, мінування або використання дронів-камікадзе. У деяких випадках сучасне озброєння, зокрема термобаричні або ракетні боєприпаси, знищує тіло повністю. У результаті – родини не отримують жодного підтвердження й вимушені жити в стані затяжної невизначеності.

Відсутність змоги ідентифікувати загиблих – одна з найгостріших проблем сьогодні. Ідентифікація тіла – це не лише про юридичний статус, а й про право родини знати правду, попрощатися, поховати близьку людину та завершити травматичну невизначеність. Водночас ця процедура потребує як технічних можливостей, так і доступу до зони бойових дій, до тіл загиблих і до відповідної інформації, якої, зазвичай, російська сторона не надає.

В Україні нині діє процедура, яка дозволяє родинам домагатися офіційного визнання смерті зниклого. Щоб зняти статус безвісти зниклого, родичі можуть звернутися до суду з позовом про встановлення факту смерті. Основою для такого рішення можуть бути докази з фронту, фото, відео, свідчення побратимів, результати експертизи ДНК або дані з реєстрів. Якщо ж підтвердження загибелі немає, але людина вважається зниклою понад шість місяців, родина може подати заяву про визнання її померлою. Стандартна тривалість

процедури – від шести місяців до року, однак на практиці через складність збору доказів та завантаженість судів вона може тривати декілька років.

У деяких випадках, щоб отримати хоч якусь відповідь, родинам доводиться вести тривалу юридичну боротьбу, звертатися до прокуратури, військових частин, архівів, комісій з питань зниклих – усе це на тлі глибокої емоційної травми. Паралельно вони стикаються з бюрократичними труднощами, відсутністю чітких механізмів комунікації та нерідко – з відчуттям залишеності. І ця проблема потребує вирішення, зокрема, і з боку держави.

Адже проблема зниклих безвісти залишається однією з найгостріших гуманітарних криз, спричинених війною. Попри зусилля України щодо збору ДНК-зразків, створення реєстрів і взаємодії з МКЧХ, системне ігнорування з боку РФ робить цю ситуацію майже нерозв'язною. Ігнорування обов'язків, передбачених міжнародними договорами, перетворює зникнення на знаряддя психологічного терору. Право родини знати правду, отримати тіло, гідно попрощатися – це не питання милосердя, це питання міжнародного права ***(https://blogs.pravda.com.ua/authors/mamedov/6823136834a46/). – 2025. – 13.05).***

***

Блог на сайті «Освіта»

Про автора: Олександр Триліс, учитель фізики, науково-дослідницька школа Базис.

Освіта для життя – хибна освітня концепція та спроба уникнення відповідальності.

Ідея переорієнтувати освіту під зрозумілі прагматичні цілі «щоб знадобилося в житті» народилася від необхідності пояснити провал попередніх реформ (у які були вкладені значні ресурси).

Чому учні у своїй масі невмотивовані до навчання, не проявляють допитливості та старанності, не показують високих результатів? Так ось чому – їх змушують вчити нудну теорію, сухі факти, розв'язувати відірвані від реальності задачі.

То давайте наповнимо програми та задачники актуальним змістом, покажемо дітям, як це все працює у житті – і разом з радісними дітьми полинемо у щасливе майбутнє.

Декілька слів, чому це погана ідея.

1. Концепція «Освіта для життя» приписує дітям прагматизм, якого вони не мають. Подивіться, як діти штовхаються, сміються, грають у футбол, у шахи, читають книжки, «втикають» у комп'ютерні ігри, лазять по деревах, стрибають через калюжі – чому вони це роблять? Як це знадобиться їм у житті? Та якщо дещо і знадобиться – чи усвідомлюють це діти? Чи є це значущою частиною мотивації? Навчіть дитину зав'язувати шнурки, мити посуд, зашити дірку на одязі, розрахувати бюджет на місяць – речі, безперечно, потрібні для життя. Чи буде це гарантовано сприйнято з ентузіазмом та захопленням?

2. «Освіта для життя» створює протиставлення, наче є гарна освіта – та, що для життя, і погана – оте все нудне. Так відмітається величезний пласт людської культури, який не має прикладного значення. Музика, абстрактна математика, поезія, живопис – все це, мабуть, баласт, бо на хліб не намажеш. Хоча ні, художник може намалювати вивіску для гастронома, а математик – порахувати прибуток від продажу масла. Музика Баха знадобилася ж для рінгтонів телефонів? Отже, для музикантів не все втрачено. Насправді те, що не має безпосереднього прикладного значення, завжди тривожило сапієнсів, чіпляло вищі форми когнітивної діяльності – і, зрештою, мало визначальний вплив на цілком прикладні питання. Закласти у фундамент відмову від ідей, які не мають прямого застосування у повсякденному житті – означає позбавити людство фантазії, мрії.

3. Вимога «освіта має давати знання, які працюватимуть у повсякденному житті» створює хибну мету. Шкільна фізика не надасть здатність ремонтувати електроприлади. Шкільна біологія не дозволить вилікувати кота. У сучасному повсякденному житті ми маємо покладатися на спеціалістів, на професіоналів.

Плекання кваліфікованого, відповідального спеціаліста – ось справжня мета, а не «дивіться діти, важіль допоможе вам підняти важкий предмет». Сучасний спеціаліст потребує обсягу знань, який важко вкласти в побутовий рівень «це знадобиться».

4. За моїми спостереженнями, є багато людей, які протиставляють «життя» та «професійну діяльність». Такий собі совковий підхід «горбатишся за гроші», а потім «живеш» – тиждень на рік у відпустці, або хоча б у п'ятницю ввечері. Деструктивний егоїстичний підхід: «життя» це для себе, а професійна діяльність – тяжкий обов'язок. У такій системі відліку виходить, що для учнів природно уникати навчання, бо це – тяжкий обов'язок, а щоб вони щось вивчили, це має бути корисно їм персонально, тут і зараз. Токсичний світогляд, але «освіта для життя» виглядає в ньому цілком привабливим. Ви не фаршируйте мою дитину нудною математикою, а навчіть її захищати свої права у суді.

Якісна освіта передбачає, звичайно, практичні навички, корисні знання, які знадобляться на побутовому рівні. От тільки рівень розуміння сучасного світу, який дозволить повноцінно реалізуватися в ньому – це значно більше. У процесі розвитку ми проживаємо багато такого, що нам потім не знадобиться. Насолоджуючись гірським краєвидом чи вивчаючи історію давньої Греції, не запитуємо себе «а навіщо це мені знадобиться».

А секрет «що треба, щоб діти вчилися» простий. Потрібна школа, яка приймає цих дітей, а не воює з ними «не списуй», «де домашнє завдання», «батьки не виховали», «сховай телефон».

Потрібні вчителі, які можуть запропонувати щось цікавіше за той же телефон. Для яких «учень не слухається» не робить учня ворогом, а є професійною задачею, з якою загалом ясно, як впоратися. Потрібні вчителі з високими когнітивними та комунікативними здібностями, от і все, і весь секрет. Ці вчителі зроблять теорію захоплюючою, факти яскравими, задачі цікавими.

Потрібні школи, у яких будуть навчати різному і по-різному, щоб можна було вибирати. І потрібна держава, яка підтримуватиме ті освітні напрямки, у яких є стратегічна потреба.

Насправді це не складно, і це, в принципі, ясно, як робити, і це – дорого (значно дорожче, ніж написати нові програми чи розробити нові критерії оцінювання). Гадаю, навіть відомо, скільки.

Чи є на це гроші – питання з розряду «чи маю я час сходити в туалет», пробачте за натуралізм ***(https://osvita.ua/blogs/94698/). – 2025. –26.05).***

***

Блог на сайті «Lb.ua»

Про автора: Петро Андрющенко, керівник Центру вивчення окупації

Велике урядове шахрайство

Черговий раз Уряд прозвітував про успішну реалізацію програми еВідновлення в частині видачі допомоги ВПО. Знову мова про 100 тисяч родин внутрішніх переселенців, які отримали допомогу. Допомогу, на фінансування якої нам дали гроші європейські партнери. Ті самі 150 млн євро. Наголошу, що саме на підтримку ВПО.

Тепер Уряд відзвітував перед європейцями про щасливі сім'ї ВПО. І можна знову просити гроші.

Але є одне але. Жоден справжній біженець, який втратив все в окупації, не отримав ані копійки з цих грошей. Жоден. Справжній ВПО. Жодної копійки.

Тоді, про що мова? Хто та головне звідки ці 100 тисяч родин, яких підтримав Уряд.

І тут саме цікаве. Давайте, з історії питання. Стисло. На відновлення України нам грошей ще не дають. Ніяких. Проте, через співчуття, партнери були готові профінансувати допомогу для ВПО. Людям, які пережили окупацію і втратили все.

Але вирішити це питання Уряд не готовий. Бо розподіляти обмежений ресурс між маріупольцями, бердянцями та мелітопольцями складно. Всі втратили, але хто перший? Кому більше? Як прописати процедуру? А якщо якось і прописати, то сотні тисяч маріупольців просто обвалять всі бюджети. Це, з одного

боку. З іншого, суто з політичної точки зору, вимушені переселенці – дуже складний електорат для влади. Незадоволений, щось вимагає і всіх проблем не вирішити. Тому голоси якщо і будуть, то дуже складно здобуті.

Інша справа – кияни, бучанці, запоріжці, дніпровці (і далі по списку). Будинки, які пошкоджено / знищено, але. Якщо їм допомогти, то вони будуть щасливі. Бо втрата "дому" як будинку – це не втрата "дому" як всього. Нажаль, через росіян тут руйнувань вистачає.

І виникла одна проблемка. Як киянина зробити ВПО, щоб отримати на ВПО гроші від європейців, але витратити не на маріупольця. А на киянина. Виклик? Авжеж.

Проте, українська бюрократія та корупція – генератор рішень. Уряд в Законі «Про облік внутрішньо переміщених осіб» зазначив, що до ВПО відносяться всі, чиє житло пошкоджено, не зважаючи на місце проживання. Цитата:

"На отримання довідки мають право особи, житлові приміщення яких знищені або пошкоджені (до ступеня непридатного для проживання) внаслідок збройної агресії Російської Федерації, що підтверджується відповідним актом обстеження технічного стану житлового приміщення (будинку, квартири), та неповнолітні діти, які отримали паспорт громадянина України, незалежно від наявності (відсутності) реєстрації місця проживання, якщо інформацію про них внесено до Єдиної інформаційної бази даних про внутрішньо переміщених осіб".

У підсумку ми отримали сотні тисяч ВПО, які ніякі не ВПО. При тому, вони мають право на участь у "еВідновлення". Плюс – до всіх інших переваг ВПО з точки зору відсутності черг в садочках, чи школах, чи іншому. Хитро? Безумовно.

Тепер маємо добру сотню тисяч задоволених псевдо-ВПО, які дозволять Уряду й далі отримувати гроші в європейців. Та з іншого боку – є потенційними виборцями влади, яка їм реально допомогла.

Все це огидно. Щонайменше. Та, безумовно, тхне не лише хитрістю, а корупцією для того хто знає як працює "еВідновлення". Мова про підрядників, ціни та схеми.

Притому, життя реальних ВПО не покращилось ані на хвилинку. Ані на копійку. Навпаки.

І це ще не всі негативні наслідки для українських біженців.

В червні міністри ЄС будуть вирішувати, що робити з мільйонами українців з березня 2026 року, коли закінчиться статус тимчасового захисту. І тут наші урядовці, які мріють всіх повернути додому, навіть якщо жити прийдеться на вокзалі, покажуть це на прикладі "еВідновлення" та використають його як аргумент. Аргумент для європейців, які зможуть примусити біженців повертатись назад в Україну.

Все це – велике урядове шахрайство, яке має бути висвітлено та покарано. І якнайшвидше, допоки ми остаточно не втратили наших біженців ***(https://lb.ua/blog/petro_andriushchenko/678792_velike_uryadove_shahraystvo_.html). – 2025. – 28.05).***

***

Блог на сайті «Освіта»

Про автора: Сергій Захарін, державний секретар Міністерства освіти і науки України (2021–2023), доктор економічних наук, професор.

Вирішення проблем природничої освіти: хайп не допоможе

Про кризу природничої освіти говорять і пишуть вже давно. Ознак цієї кризи багато: незадовільний рівень матеріально-технічного забезпечення лабораторій та спеціалізованих аудиторій у закладах освіти; недостатня кількість сучасних навчально-методичних матеріалів (у тому числі інтерактивних); дефіцит вчителів, що викладають природничі предмети; відсутність витратних навчальних матеріалів (реактивів) тощо.

Але ключовий прояв кризи, на мій погляд, полягає в недостатній кількості мотивованих здобувачів (учнів, слухачів, студентів, аспірантів), які бажають глибоко опановувати природничі науки. Економісти в таких випадках кажуть: немає попиту…

Автору цих рядків здавалося, що про проблему – як мінімум – знають в освітньому відомстві. А тому – як мінімум – розуміють необхідність та шляхи її вирішення. Але освітні управлінці інколи пропонують, скажімо так, «занадто дивні» шляхи, які нагадують «махрову радянщину».

Заступник міністра освіти і науки України Михайло Винницький в інтерв'ю інтернет-виданню «Дзеркало тижня» розказав, що для здачі національного мультипредметного тесту (НМТ) зареєструвалося 312 тисяч учасників, кожен з яких міг обрати четвертий предмет на свій розсуд. Пряма мова: «Близько 115 тисяч осіб (це більш як третина) обрали четвертим предметом англійську мову. Ще 73 тисячі обрали географію, 62 тисячі – біологію, 46,5 тисячі – українську літературу. І, на жаль, найменше учасників обирали фізику та хімію: фізику – майже 9 тисяч, а хімію – майже 3 тисячі. Це дуже прикро, адже фізика та хімія – дуже важливі предмети, які фактично забезпечують природничу галузь, інженерію, технології».

Ця тенденція – найменша кількість абітурієнтів, які обирають фізику і хімію в якості предмета для здачі НМТ – спостерігається вже кілька років. Вочевидь, випускники не бажають обирати ці предмети через дефіцит відповідних знань.

Як наслідок – серед основної маси здобувачів вищої освіти (у тому числі і тих, які опановують так звані «природничі» спеціальності), відчувається брак знань (у тому числі елементарних) з природничих наук, особливо з фізики і хімії.

Нещодавно я спілкувався з викладачами медичного університету. Вони звернули увагу на таку обставину: в академічній групі, в якій навчається 25–30 студентів, лише двоє чи троє здавали на НМТ хімію. У результаті, лише 2–3 здобувачі освіти можуть зрозуміти навчальну програму першого курсу хоча б на базовому рівні. Іншим здобувачам доводиться викладати елементарні теми із шкільного курсу хімії. І далеко не завжди здобувачі – майбутні лікарі – добре засвоюють навіть ці елементарні теми.

Пан Винницький не лише визнає наявність проблеми, а навіть визнає, що її треба вирішувати: «Це велика проблема, з якою ми маємо довгостроково працювати, адже відмова від вивчення фізики та хімії відбувається не на етапі вступу до вишів, а набагато раніше. Цього року ми впровадили інновацію в Порядок прийому на навчання: ті абітурієнти, які обирають фізику або хімію як четвертий предмет, отримують певні переваги під час вступу. Для осіб, які обирають ці предмети, передбачено спеціальний метод підрахунку конкурсного балу».

Отже, виходить, ключовий інструмент «популяризації» природничих наук серед учнів – це не нові підручники, не нові лабораторії, не інтерактивні методи, не сучасні мотивовані вчителі, а «метод підрахунку».

Що ж це за «диво-метод»?

Відповідь заступника міністра: «Конкурсний бал за НМТ у вступника, який обрав один із цих двох предметів і вступає на природничу або інженерну спеціальність, буде вищим, ніж у вступника, який обирає ту саму спеціальність, але з іншим вибірковим предметом (за рівних результатів із трьох обов'язкових). Конкретний рівень переваги залежатиме від обраної спеціальності: для природничих – більша, для інженерних – трошки менша, для соціально-економічних – іще менша. Але все ж таки перевага буде, й це інновація, яку запроваджено саме цього року в Правилах вступу-2025. Та очевидно, що цьогорічні вступники почали готуватися до НМТ ще задовго до того, як її було оприлюднено. Тому ми плануємо надавати перевагу під час вступу тим, хто обирає фізику або хімію, й наступного року, й за рік».

За задумом стратегів, які постійно перелаштовують освітню політику, видумуючи все нові і нові правила, вказаний «метод» – пільга при вступі – має сформувати у дітей стійку мотивацію до вивчення фізики і хімії. Тобто, ще за кілька років до вступу школяр або школярка мають розпочати заповзято вивчати ці дисципліни – для того, аби під час здачі іспиту отримати так званий «конкретний рівень переваги».

На мій погляд, обрано занадто простий, можна навіть сказати – примітивний метод вирішення проблеми. Здається, такий метод

дозволяє скоріше дати швидку відповідь на заздалегідь заготовлене запитання журналістки, аніж «по-справжньому» проблему вирішити.

Для того аби вирішити проблему «по-справжньому», необхідно вивчити її причини на глибинному рівні, а також залучити до її вирішення справжніх фахівців. «Агенти та агентки змін», «освітні експерти та експертки», «незалежні ментори» з грантових проєктів – це все весело, вигідно і чудово, але інколи слід слухати і думку професіоналів.

Півтора роки назад було оприлюднено результати Міжнародного дослідження якості освіти PISA (Program for International Student Assessment). З наявних даних вбачається, що у 2022 році українські учні продемонстрували гірші результати, аніж у 2018 році; гірші результати, аніж учні переважної більшості країн ОЕСР; гірші результати, аніж середньосвітові.

Українські школярі в середньому набрали 450 балів за шкалою з природничо-наукових дисциплін. Середній показник у світі – 485. Найкращий – у Сингапурі: 561.

Показово, що у 2018 році українські школярі набрали в середньому 469 балів, відстаючи від середнього значення розвинутих країн лише на 4%.

Дві третини українських школярів, які брали участь у дослідженні 2022 року, показали низькі або вкрай низькі результати з природничих дисциплін (рівні 1 та 2, а усього рівнів – 5). Рівень «5» продемонстрували лише 2% українських школярів, а середній показник у світі (включаючи бідні країни) – 6,3%.

Зазвичай завдання з природничих наук в дослідженні PISA є когнітивно складними, під час їхнього розв'язання не вимагається наявності великого обсягу фактичних даних. Аби дати правильну відповідь, необхідно знати лише невеличку кількість базових фактів (законів, закономірностей), і вміти їх використовувати для пояснення різних природних явищ і процесів. Докладніше про це – тут.

Автори звіту PISA-2022 навели десять прикладів завдань, які було поставлено учням під час дослідження. Сумлінні вчителі та методисти, опрацювавши цей матеріал, можуть більш чітко зрозуміти – на що саме слід звернути увагу під час викладання природничих дисциплін.

Під час дослідження компетентностей з природничих наук учням ставили доволі оригінальні завдання: із загальної хірургії, організації функціонування рибної ферми, методик спостережень за міграцією птахів, щодо роботи агрегатів автомобіля, проблем куріння, бігу у спекотну погоду, принципу апарату ультразвукової діагностики. Усі ці теми в українській школі не вивчають або майже не вивчають, але дати правильні відповіді можна, якщо вміти застосувати отримані знання на практиці.

PISA-2022 показало ключову проблему змісту природничої освіти в українській школі – теоретичність, абстрактність, відірваність від практики, перевантаженість відірваними один від одного фактами, неспроможність сформувати у здобувачів основи критичного мислення (принаймні, відносно природних явищ і процесів).

Звідси – сприйняття здобувачами природничих дисциплін (в першу чергу фізики і хімії) переважно як «книжного знання», яке неможливо перевірити або застосувати в «справжньому» житті.

У світі, де панують інформаційні технології, а суспільство стає мережевим, у людини (у тому числі дитини) поступово втрачається мотивація вивчати щось «абстрактне і книжне», натомість є потреба у опануванні практично орієнтованих компетентностей.

Ми можемо довго дискутувати – добре це чи погано – але результати навчання, безсумнівно, залежать від мотивації, а мотивація в свою чергу в значній мірі залежить від суспільних настроїв.

Чи слід дивуватися, що наші учні не проявляють великої цікавості до вивчення предметів природничого спрямування? Чи слід дивуватися, що випускники шкіл в переважній більшості випадків не обирають фізику і хімію як предмети, що можна здавати під час НМТ?

У звіті PISA-2022 аргументовано і доказово описані ключові інституційні проблеми,

які перешкоджають школярам опановувати навчальний матеріал на належному рівні:

значно менші, аніж у розвинутих країнах, освітні витрати (у перерахунку на одного учня);

брак навчальних матеріалів – підручників, комп'ютерів, лабораторного обладнання (на це вказали керівники закладів, у яких навчаються 75% учнів, що взяли участь у дослідженні);

низька якість наявних навчальних матеріалів (70%);

брак освітньої інфраструктури – відсутність сучасних навчальних корпусів, спортивних майданчиків, інженерних мереж (52%);

брак або низька якість цифрових ресурсів (75%);

суттєвий дефіцит педагогічних кадрів (на це вказали 30% керівників шкіл);

неналежна або низька кваліфікація педагогічних кадрів (на це вказали 22%);

падіння рівня охоплення учнів дошкільним навчанням.

Заступник міністра, нагадаю, говорить не про удосконалення змісту освіти і не про облаштування лабораторій (бо це не популярно у соціальних мережах), натомість говорить про новий «метод» підрахунку балів (бо це швидке рішення, швидка відповідь на «паркетне» запитання, і плюс – можна швидко заробити купу лайків).

І наостанок – деякі професорські роздуми.

Ключові параметри політики у сфері доступу до вищої освіти щорічно змінюються – інколи цю забаву називають «візіюванням» або «дизайнуванням». Регулярно проводяться яскраві форуми (з іноземними гостями і дорогими фуршетами), на яких презентуються візії, місії і слогани.

І ми, прості освітяни, до цього вже звикли. Але було б бажано, аби освітні проблеми вирішувалися не лише нескінченним «дизайнуванням» формул, підходів, методів і моделей, а в першу чергу – шляхом змістовного вирішення базових проблем.

Керівники освітньої системи, на жаль, не демонструють лідерства у подоланні цих проблем.

Приміром, 2 квітня на сайті освітнього відомства оприлюднено новину із яскравим заголовком: «Освіта для життя: МОН розпочинає оновлення змісту природничої освітньої галузі».

Зі змісту новини стало відомо, що на 8 квітня 2025 року було заплановано «відкриту дискусію» про майбутнє природничої освіти в Україні. «Концепцію природничої освітньої галузі, яка є однією з пілотних галузей на наступний навчальний рік, разом із концепціями інших освітніх галузей буде презентовано громадськості навесні 2025 року. Практичне впровадження змін розпочнеться восени для учнів і учениць 5 класів у мистецькій, природничій та технологічній галузях. У межах реформи також передбачено модернізацію лабораторій у закладах загальної середньої освіти», – написано на сайті.

Боюся помилитися, але українській освітній спільноті знову в якості результату запропонують… презентацію. Вочевидь, за задумом «ідеологів освітніх змін», ми маємо почитати презентацію і очманіти от «невтомного служіння» нинішньої бравої «освітньої команди». Навіть якщо в презентації будуть написані «правильні слова» – це ще не означає, що освітні управлінці посеред бюджетного року знайдуть необхідні гроші, аби ці «правильні слова» починати впроваджувати в школі вже зараз.

Взагалі, не зовсім розумію – чи потрібно нескінченно обговорювати якісь проблеми, нескінченно формулювати пропозиції і рекомендації, нескінченно щось «дизайнувати», якщо конструктивні пропозиції вже були сформульовані півтора роки назад авторами авторитетного міжнародного дослідження.

Показово, що вже наявні пропозиції і рекомендації – не імплементуються, натомість «штампуються» все нові і нові презентації.

Ми, прості освітяни, очікуємо на серйозне і вдумливе вирішення проблем, а не хайп, гасла, лайки і презенташки. Усе менше і менше сподівань, що нинішні «освітні генерали» здатні задовільнити наші природні очікування ***(https://osvita.ua/blogs/94711/). – 2025. – 28.05).***

***

Блог на сайті «Lb.ua»

Про автора: Дмитро Лубінець, уповноважений Верховної Ради України з прав людини

Соціальна нерівність в гірських громадах: чому ВПО не отримують належні доплати?

У зв'язку зі збройною агресією РФ проти України багато внутрішньо переміщених осіб знайшли тимчасовий прихисток саме в західних регіонах України. Проте ВПО на сьогодні не мають рівного доступу до соціальних гарантій, як місцеві жителі, зокрема, до "гірських доплат".

Станом на жовтень 2024 року 70 665 осіб зі статусом ВПО проживають у гірській місцевості понад шість місяців (за інформацією ДП "Інформаційно-обчислювальний центр Міністерства соціальної політики України").

Кількість населених пунктів зі статусом гірських у західних регіонах України є наступною: Івано-Франківська область – 242, Закарпатська область – 214, Львівська область – 196, Чернівецька область – 64.

Чому гірський статус важливий?

Зазначу, що відповідно до Закону України "Про статус гірських населених пунктів в Україні" статус особи, яка має право соціальні гарантії як мешканець гірської місцевості, може бути надано тим, хто:

постійно проживає на території гірського населеного пункту;

постійно працює на території гірського населеного пункту (навіть якщо підприємство, установа, організація розташовані за межами населеного пункту, якому надано статус гірського, але мають філії, представництва, відділення, інші відокремлені підрозділи і робочі місця в гірських населених пунктах);

навчаються на денному відділенні у навчальному закладі, який знаходиться у гірському населеному пункті;

окремим особам інших населених пунктів та тим, які проживають за межами населених пунктів, умови проживання яких відповідають критеріям віднесення населених пунктів до гірських та особам, які постійно працюють або несуть службу на лісогосподарських підприємствах, гідрометеорологічних станціях, заставах, обсерваторіях, інших об'єктах, що розташовані поза межами гірських населених пунктів.

Які переваги дає гірський статус

Пенсії, стипендії, всі види державної матеріальної допомоги збільшується на 20 відсотків. Тарифні ставки та посадові оклади працівників підвищуються на 25 відсотків за умови, що робоче місце розташоване в населеному пункті, якому надано статус гірського.

У чому полягає проблема?

На сьогодні існує правова колізія при одночасному застосуванні Закону України "Про забезпечення прав і свобод ВПО" та Порядку оформлення і видачі довідки про взяття на облік ВПО.

Проблема полягає в тому, що поняття "постійне проживання" не визначене чітко, і місцева влада часто трактує його лише як наявність реєстрації, нехтуючи фактичним проживанням.

Зазначу, що така ситуація порушує вимогу "якості закону", що передбачена Європейською конвенцією з прав людини. У випадках, коли є кілька тлумачень норм, закон має застосовуватись у спосіб, найбільш сприятливий для особи.

Відповідно до статті 5 Закону України "Про забезпечення прав і свобод внутрішньо переміщених осіб" довідка про взяття на облік внутрішньо переміщеної особи засвідчує місце її проживання на період наявності підстав, які призвели до внутрішнього переміщення.

Що я рекомендую, як Омбудсман України? Звернути особливу увагу на законопроєкт №13237 від 30.04.2025 "Про соціальний захист осіб, які проживають, навчаються на території гірського населеного пункту, який потребує додаткової підтримки". Документ має важливе соціальне значення, адже його ухвалення дозволить вирішити проблему нерівного доступу до соціальних гарантій для ВПО у гірських регіонах.

Закликаю ВПО звертатися до органів місцевої влади, Центрів надання адміністративних

послуг, сільських, селищних чи міських рад, які уповноважені приймати рішення про надання відповідного статусу, оскільки наявність довідки про взяття на облік ВПО, підтверджує фактичне місце проживання особи ***(https://lb.ua/blog/dmytro_lubinets/678954_sotsialna_nerivnist_girskih.html). – 2025. – 29.05).***

***

Блог на сайті «Українська правда»

Про автора: Андрій Боровик, виконавчий директор Transparency International Ukraine

Дорожні карти в Європу

Євроінтеграція України – це непростий шлях. При підготовці до далекої поїздки люди попередньо вивчають маршрут, тож очевидно, що для тривалого шляху великої країни теж потрібно розібратися у напрямах руху та визначитися з конкретним планом дій. І Україна такий план уже має.

Минулого тижня Кабмін затвердив три важливі документи, які мають стати основою для євроінтеграції України – Дорожні карти трансформацій у сферах верховенства права, реформи державного управління та функціонування демократичних інституцій. Погодження цих документів має нарешті дати старт перемовинам про вступ України в Євросоюз.

Що ж дадуть ці дорожні карти нам після прийняття? Спробуємо розібратися.

Взагалі дорожня карта – це документ, у якому країна-кандидат визначає ключові реформи в конкретній сфері та встановлює строки їх реалізації.

Тобто це такий собі збірник, в якому сформульовані конкретні проблеми функціонування країни, які заважають їй повноцінно інтегруватися в Євросоюз, а також розписаний детальний план того, як надалі ці проблеми долатимуться.

Але це не єдина функція дорожньої карти, адже такий документ також слугує основою для моніторингу прогресу країни-кандидата з боку Європейської Комісії.

Тож, перш ніж розпочати процес переговорів з ЄС про вступ, кожна країна-кандидатка має розробити і погодити з Єврокомісією такі дорожні карти.

От і Україна у межах вступу до ЄС підготувала три такі стратегічні документи, в яких виписані наші подальші реформи у сферах верховенства права, реформи державного управління та функціонування демократичних інституцій. І надалі під час переговорного процесу ЄС оцінюватиме готовність України до вступу зокрема за нормативними, інституційними та адміністративними критеріями.

При цьому усі ухвалені Кабміном дорожні карти синхронізовані з нашими міжнародними зобов'язаннями та іншими стратегічними документами України.

Затвердження дорожніх карт у сфері верховенства права та реформи державного управління є умовою відкриття перемовин про членство в ЄС з Україною, тобто Кластера 1 «Основи процесу вступу до ЄС» (Fundamentals).

І тут для нас особливо цікава саме дорожня карта у сфері верховенства права, адже вона охоплює майбутні реформи у системі правосуддя, антикорупційній системі, сферах плюралізму і свободи ЗМІ, а також інші інституційні питання, пов'язані з системою стримувань і противаг.

Дорожню карту з верховенства права український уряд прийняв на основі вказівок, наданих у звіті про результати перевірки Європейською Комісією. Тут важливо, що фінальний текст цього документа – це результат тривалої роботи усіх зацікавлених сторін.

Після прозорого процесу змістовних консультацій між українською владою та європейськими партнерами, із якісним залученням експертів від громадянського суспільства, у тому числі й TI Ukraine, країна отримала значно кращий варіант дорожньої карти ніж перші версії цього документа. Зокрема, творці документа врахували наші рекомендації щодо проведення конкурсу ВАКС із залученням ГРМЕ, вдосконалення строків давності та механізмів процесуального контролю у корупційних справах. І, звісно, важливим досягненням є врахування пропозицій щодо запровадження відповідальності прокурорів за порушення підслідності.

Проте є й важливі речі, які, на жаль, не були враховані в дорожній карті. Наприклад, пропозиції надати надання керівнику САП можливості ініціювати провадження та погоджувати слідчі дії щодо народних депутатів. А ще в документі не вказано про необхідність запровадити конкурс на посаду Генпрокурора та створити конкурсні комісії з участю міжнародних експертів для добору керівників правоохоронних органів.

Не повністю враховані також рекомендації щодо розробки системи моніторингу тривалості розслідування та судового розгляду корупційних справ, удосконалення механізмів управління арештованими активами та заборони блокування такого управління через рішення судів некримінальної юрисдикції. І так само залишились без суттєвих змін і можуть бути вдосконалені заходи у сфері публічних закупівель.

Тут важливо, що низка важливих ініціатив у документі запланована лише на 2027 рік, що може уповільнити процес євроінтеграції та реформування системи кримінальної юстиції. Проте такі недоліки таки можуть ще врахувати, адже впровадження цієї дорожньої карти буде постійно контролюватися та регулярно розглядатися на міжурядових конференціях протягом усього процесу нашої євроінтеграції.

До кінця 2027 року, коли закінчуються терміни, прописані в дорожній карті, Єврокомісія уважно стежитиме за прогресом України в усіх сферах. І використовуватиме для цього всі доступні інструменти. Це можуть бути експертні виїзні перевірки з боку Комісії та держав-членів, діалог у рамках Угоди про асоціацію, включаючи поглиблену та всеосяжну зону вільної торгівлі, та показники третіх сторін, де це доречно.

При цьому Єврокомісія регулярно інформуватиме Раду ЄС про прогрес України в будь-якій галузі під час переговорів, і зокрема під час представлення проєктів спільних позицій ЄС.

Дорожні карти ухвалили, і що далі?

Формально процес мав би відбуватися так.

Україні надсилають офіційний лист-запрошення, погоджений всіма членами ЄС, із запитом на отримання погоджених урядом дорожніх карт по верховенству права і реформі державного управління.

Європейська Комісія оцінює ці документи, після чого країни-члени ЄС одноголосно схвалюють дорожні карти.

Проте у випадку з Україною все інакше. Бо Угорщина проти.

Через блокування з боку Угорщини, лист-запрошення нам так і не надіслали, тому Україна прийняла рішення не чекати юридичного погодження з Брюсселю, а затвердила дорожні карти зі свого боку. Ці кроки повністю погоджені із владою ЄС і є частиною того самого «плану Б», про який не так давно говорила Кая Каллас, і який так добре описали у своїй статті журналісти «Європейської правди».

Але, хоч позиція уряду Віктора Орбана і гальмує весь процес нашої інтеграції в Євросоюз, потреба впроваджувати якісні реформи нікуди не зникне – адже без таких змін вступити в ЄС не вийде. Тому, маючи конкретний план, можна і варто діяти вже зараз, адже хто іде – той і дійде ***(https://blogs.pravda.com.ua/authors/borovyk/68380afba3548/). – 2025. – 29.05).***

***

Блог на сайті « Lb.ua»

Про автора: Ірина Славінська, співзасновниця ДонорUA та Президентка ГО «Всеукраїнська асоціація донорів України»

Пільги для донорів крові: наріжний камінь реформ

Цього року втрачають чинність деякі пільги для донорів крові. Багато людей занепокоєні тим, що такі зміни призведуть до зменшення кількості регулярних донорів. Активісти зареєстрували вже не одну відповідну петицію, аби повернути донорам пільги, й часто звертаються до ДонорUA з проханням підтримати ініціативу. Проте ми як профільна організація, що популяризує донорство крові, не можемо цього зробити, оскільки система безоплатного, волонтерського донорства – шлях для вступу України в ЄС. Розберемося, як це працює.

Які саме пільги скасовують і чому?

Згідно з Законом України "Про безпеку та якість донорської крові та компонентів крові", втрачають чинність такі пільги:

додатковий вихідний для донорів (право на вихідний у сам день донації залишається);

допомога в разі тимчасової непрацездатності у зв'язку з захворюванням;

надбавка до стипендії для донорів-студентів;

надбавка до пенсії для Почесних донорів.

Пільги втрачають силу через 5 років після введення Закону в дію. Опублікували його 30 вересня 2020 року, чинності він набрав наступного дня, і був введений у дію через 3 місяці після цього. Отже, з 31 грудня цього року пільги мають бути скасовані. Проте, якщо донори встигли набути право на допомогу чи надбавку раніше, вони ці пільги не втрачають.

Закон розробили, аби адаптувати законодавство України до європейської правової системи у межах виконання Угоди про асоціацію між Україною та ЄС.

У ЄС стандарти якості та безпеки донорської крові визначає відповідна Директива:

"Добровільне та безоплатне донорство крові є фактором, що може сприяти високим стандартам безпечності крові та її компонентів, і, відповідно, охороні здоров'я людини. Необхідно підтримувати зусилля Ради Європи у цій галузі, а також вживати всіх необхідних заходів для заохочення добровільного і безоплатного донорства за допомогою відповідних заходів та ініціатив, а також шляхом забезпечення отримання донором більшого суспільного визнання, що тим самим збільшить самозабезпечення. Необхідно взяти до уваги означення добровільного та безоплатного донорства, запропоноване Радою Європи".

Згідно з дослідженнями, кров системних донорів, яку вони здають добровільно й безоплатно, є безпечнішою. Коли донор шукає вигоди, вища ймовірність, що людина приховає наявність інфекцій, аби отримати винагороду. Проте й безоплатне стихійне донорство може нести ризики. Наприклад, коли наші друзі терміново шукають кров для хворої дитини, і ми хочемо допомогти, через хвилювання та поспіх ми можемо не знати або не згадати про свої протипоказання. Тому в донорстві важливий системний підхід, і альтруїзм є його невід'ємною частиною.

Коли кров чи її компоненти потрібні, аби тут і зараз врятувати життя, важлива їхня наявність, а не потенційна ймовірність, що завтра ваші друзі будуть здавати кров. Проте важливо, щоб люди долучались до донорства не лише тоді, коли хтось помирає, адже за таких умов існує ризик здачі крові під моральним чи матеріальним тиском. Планова донація – це найкраща донація. Системність надає найбільше можливостей для порятунку життів.

Відсутність пільг входить у поняття добровільності й безоплатності. Головною мотивацією донора має бути бажання допомогти – тільки в цьому випадку можна розраховувати на максимально відповідальне ставлення, а отже, й на безпечність крові. За даними ВООЗ, 79 країн збирають понад 90% донорської крові шляхом добровільного безоплатного донорства.

Практики заохочення донорів у країнах ЄС та в Україні

Винагородження за донорство крові – тема дискусійна. Доведено, що практика платного донорства підсилює нерівність у суспільстві: в африканських країнах донори з низьким рівнем доходу здають кров, отримуючи гроші від сімей реципієнтів з вищим рівнем достатку, тоді як малозабезпечені пацієнти потерпають від браку крові, оскільки безоплатне донорство розвинене слабко.

Більш абстрактний, проте не менш важливий аргумент проти платного донорства – приниження людської гідності. На думку дослідників, плата за кров дегуманізує та знецінює людину, зводячи її до джерела ресурсів. Окрім того, ця практика негативно впливає на репутацію донорства як такого і перешкоджає розвитку добровільного безоплатного донорства.

Проте в деяких країнах – наприклад, Хорватії, Чехії та Італії – все ж існують практики додаткового заохочення донорів. Переважно це негрошові винагороди – наприклад, додаткові вихідні. Значну роль у популяризації донорства відіграють громадські

організації: організовують тематичні події, дарують донорам мерч або інші подарунки. Проте суть не в тому, аби заплатити донору за кров – грішми чи будь-чим іншим – а в тому, аби закріпити позитивний досвід і підсилити інтерес. Заохочення не повинне бути настільки значним, аби стати ключовою мотивацією до донорства.

ДонорUA розвиває та популяризує донорство крові в Україні вже 10 років. Ми застосовуємо комплексний підхід, який включає в себе:

відкриті виїзні донації як спосіб популяризації та закриття термінових точкових потреб у крові;

корпоративне донорство для підвищення КСВ компаній та формування культури донорства через вплив бізнесу;

безкоштовні відкриті акції з визначення груп крові, які привертають увагу до теми донорства;

бонусну програму: подарунки та знижки від партнерів у якості подяки за донацію крові;

щорічне нагородження Почесних і Заслужених донорів.

Відмінність між пільгами і бонусами – у масштабі. Навряд чи хтось здасть кров саме для того, аби отримати знижку 15% на книжки. І точно ніхто не здаватиме її 40 чи 100 разів, щоби їм подарували грамоту. Наша мета – не "купити" донора, а подякувати та подарувати гарний настрій.

Чи справді Україні потрібні пільги для донорів?

Аргументи на користь пільг, які ми зустрічаємо в мережі, часто зводяться саме до соціальної нерівності. Люди хочуть мати право на додатковий вихідний, аби наступного дня після донації не довелося важко фізично працювати. Їм потрібна допомога на випадок хвороби, оскільки не всі мають змогу зі своєї зарплатні відкладати гроші на такі випадки. Годі й говорити про надбавку до пенсії, розмір якої часом дозволяє лише сплатити комунальні послуги.

Право на відпочинок і гідне ставлення до здоров'я, соціальні гарантії та гідна пенсія – те, що мало би бути у всіх. Але не система крові повинна вирішувати питання низьких зарплат і пенсій. Це комплексна проблема, яку неможливо усунути пільгами. Вони справді лише нормалізують і підкреслюють нерівність.

Здавати кров слід за покликом серця. А для того, аби цей поклик відчували якомога більше людей, необхідно популяризувати добровільне й безоплатне донорство на рівні держави та спільнот. Провадити інформаційні кампанії, модернізувати систему крові, аби донорство ставало простішим і доступнішим. І все це відбувається, хоч і не такими темпами, як усім нам би того хотілося.

Хай там як, а головною мотивацією для донорства був і лишається порятунок життів. Кожна третя людина у світі може потрапити у ситуацію, коли потребуватиме донорської крові. Сьогодні ми здаємо кров і розповідаємо іншим, як це важливо, і завтра можемо розраховувати, що і для нас вона знайдеться, якщо виникне потреба. А потреба ця під час повномасштабної війни гостра, як ніколи. Донація – безцінна допомога пораненим бійцям на фронті і найкраща підстраховка на випадок обстрілів цивільних об'єктів. Крові потребують травмовані рятувальники, мами під час важких пологів, діти з онкозахворюваннями, постраждалі на виробництвах і тисячі інших пацієнтів. І їхні життя важливіші за грошову винагороду ***(https://lb.ua/blog/iryna_slavinska/679002_pilgi_donoriv_krovi_narizhniy.html). – 2025. – 30.05).***

***

Блог на сайті «Цензор.НЕТ»

Про автора: Олена Кочура, головна експертка з реформування пенітенціарної системи та пробації Проєкту ЄС "Право-Justice"

Пробація – шанс для неповнолітніх: чому суспільство має підтримати реформу правосуддя, дружнього до дитини

30 травня Президент України Володимир Зеленський підписав Указ, яким переніс День захисту дітей з 1 червня на 20 листопада – Всесвітній день дитини. Цей день зазвичай асоціюється з подарунками, святковими заходами та гучними промовами про права дитини. Та за цією поверхневою

ритуальністю легко губиться тиша – тиша довкола тих підлітків, які вже стоять на межі між дитинством і кримінальним світом. Вони не з'являються на світлинах із кульками, не беруть участі в концертах і флешмобах. Про них незручно згадувати на офіційних трибунах. Але саме ці діти потребують уваги найбільше. І заслуговують не на вирок – а на шанс.

Цей шанс уже існує – і він працює. Ідеться про систему пробації для неповнолітніх, яка довела свою ефективність: допомагає дітям усвідомити провину, компенсувати шкоду, пройти шлях змін – без тавра «злочинець», без ізоляції від суспільства. Пробація в Україні – це не новація і не експеримент, а реальна частина системи правосуддя, дружнього до дитини, яка щороку дає сотням підлітків змогу обрати інший життєвий шлях. Саме тому сьогодні важливо говорити про її подальший розвиток та ширше впровадження.

Діти як дзеркало нашої дійсності

Суспільство часто очікує від підлітків дорослої поведінки, забуваючи, що їхня психіка ще не сформована, а цінності – лише в процесі становлення. Особливо гостро це відчувається зараз, у воєнний час, коли дитинство втрачає стабільність, а ризики – лише зростають.

Варто розуміти, що дитяча злочинність – не просто статистика. Це симптом глибших соціальних проблем: розірваних родинних зв'язків, економічної скрути, психологічної напруги в родинах, нестачі якісного дозвілля та належної уваги з боку дорослих. Діти – лакмусовий папірець нашого суспільства. Їхні вчинки часто є прямим наслідком того, що відбувається довкола. Коли батьки на фронті або змушені боротися за виживання, коли школа не може замінити живе спілкування через тривоги та дистанційне навчання – дитина шукає опору у вулиці, однолітках, соцмережах, а іноді й у хибних авторитетах.

Нещодавнє дослідження «Кримінологічна характеристика та запобігання кримінальним правопорушенням, вчиненими неповнолітніми» свідчить, що у 2023 році відбулося помітне зростання кількості правопорушень. Збільшилася частка тяжких злочинів. З'явилися нові правопорушення – від підпалів до насильницьких дій та співпраці з ворогом. Діти діють імпульсивно, часто не усвідомлюючи наслідків. Але це не означає, що суспільство має лише карати. Навпаки – слухати, розуміти та підтримувати.

Європейський вибір – це правосуддя з людським обличчям

У Європейському Союзі давно усвідомили, що каральна система не працює для дітей. У багатьох країнах ЄС впроваджено принципи правосуддя, дружнього до дитини – без стигматизації, без ізоляції, з фокусом на реабілітацію та ресоціалізацію. Зокрема, це вже працює у Франції, Нідерландах, Швеції – там дитину не кидають у в'язницю, а повертають до життя.

Такий підхід це не про вседозволеність чи м'якість покарань – це про ефективність, гуманність і профілактику. Зі свого боку, Україна, що прагне європейської інтеграції, взяла на себе зобов'язання впроваджувати підходи правосуддя, дружнього до дитини. На сьогодні підлітки, які вчинили нетяжкі кримінальні правопорушення, можуть бути залучені до програм відновного правосуддя ще на етапі досудового розслідування. Головна мета такого підходу – не покарання, а усвідомлення своєї провини, компенсація завданої шкоди та робота з причинами правопорушення.

Один із учасників правосуддя, дружнього до дитини, – пробація. Це альтернатива класичному кримінальному переслідуванню. Це – шанс на виправлення без тавра «злочинець».

Пробація – це не «поблажка», а дієвий інструмент змін. У кожній справі складається досудова доповідь, яка дозволяє суду побачити справжнє обличчя дитини: її життєву історію, обставини, що призвели до хибного вчинку, та її мотивацію. Це – голос дитини в залі суду. Це – можливість пояснити, що сталося і чому.

Допомогти – не значить виправдати

До реформи пробації все зводилося до формальних довідок: «вчиться – не вчиться», «характеристика позитивна – негативна». Дитину, яка оступилася, часто просто виштовхували з освітнього середовища, позбавляючи останніх шансів на зміну.

Сьогодні ж пробація працює у тісній зв'язці з родиною, школою, громадськими організаціями. Розробляється індивідуальний план роботи із кожною дитиною. Йдеться не лише про контроль, а про вплив на цінності, мислення, соціальне оточення дитини.

Приклад з життя: хлопець вкрав металобрухт у сусідів. На перший погляд – кримінальне правопорушення. Але згодом, коли фахівці почали розбиратися, з'ясувалося: він хотів продати метал, щоб купити дрова й обігріти дім. У родині – хворі батьки, безробіття, холод. Натомість завдяки пробації дитина не опинилася за ґратами. Їй допомогли вступити до професійно-технічного навчального закладу, дали дах над головою, допомогли знайти роботу. Тепер вона на іншому шляху. І це – переваги системи, яка бачить не лише провину, а й причини.

Відповідальність – шлях до змін

Так, діти мають відповідати за свої вчинки. Але головне – щоб вони змогли виправити помилку і не повторити її. Зокрема, у 2023 році понад 98% підлітків під час перебування під наглядом пробації не скоїли повторних кримінальних правопорушень. Це – не цифри. Це – долі.

Також неймовірно важливою є участь батьків або осіб, які їх замінюють. Якщо родина відмовляється від діалогу з пробацією під час підготовки досудової доповіді – дитина втрачає шанс. Суд не бачить усієї картини без родини. Тому батьки мають бути активними – не боятися говорити, пояснювати, співпрацювати. Під час перебування на пробації їхня участь та підтримка не менш важлива. Батькам варто усвідомити, що пробація – для них партнер, а не контролер.

Водночас, суспільство має усвідомити, діти, які оступилися, не зникають після вироку. Вони живуть серед нас. І якщо їм не простягнути руку сьогодні – завтра вони можуть обернутися злом. Суспільство, яке карає, але не дає шансу, вирощує озлоблених, не зламаних.

Україна має послідовно рухатися шляхом продовження реформи правосуддя, дружнього до дитини. Завдання на наступні роки – масштабувати застосування пробації, підвищувати довіру до цієї гуманної й ефективної моделі. І ця довіра має зміцнюватися через постійний діалог із суддями, адвокатами, громадами – усіма, хто приймає рішення або впливає на долю дитини.

Інвестиції в пробацію та розвиток правосуддя, дружнього до дитини, – це вклад у безпечне й людяне майбутнє. Справді європейська держава – та, що не кидає дітей за ґрати, а простягає їм руку. Та, де право суддя не мститься, а створює можливості для змін ***(https://censor.net/ua/blogs/3555250/zelenskiyi-peren-s-den-zahistu-d-teyi-z-1-chervnya-na-20-listopada-vsesv-tn-yi-den-ditini) –– 2025. – 30.05).***

***

Блог на сайті «Zaxid.Net»

Про автора: Олег Мицик, керуючий партнер у Адвокатське об'єднання «Мицик, Кравчук і Партнери»

Законодавство дозволяє мобілізацію обвинувачених за всіма статтями ККУ: *Коментар щодо мобілізації для уникнення кримінальної відповідальності*

14 квітня 2022 року Верховна Рада України прийняла Закон (набрав чинності 01.05.2022 року), яким внесено зміни до ст. 335 КПК України та викладено дану статтю в наступній редакції: «У разі якщо обвинувачений ухилився від явки до суду, захворів … або був призваний для проходження військової служби за призовом під час мобілізації, на особливий період, суд зупиняє судове провадження стосовно такого обвинуваченого до його розшуку, видужання або звільнення з військової служби і продовжує судове провадження стосовно інших обвинувачених, якщо воно здійснюється щодо декількох осіб».

Зважаючи на формулювання диспозиції статті, законодавцем визначено можливість мобілізації обвинувачених по всіх складах кримінальних правопорушень, передбачених КК України, на відміну від ст. 81-1 КК України, якою передбачено можливість умовно-дострокового звільнення від відбування покарання для проходження

військової служби. У статті 81-1 КК України, наприклад, визначено, що таке звільнення неможливе у випадку умисного вбивства двох і більше осіб, особливо тяжких корупційних правопорушень, порушення ПДР у стані сп'яніння, яке спричинило смерть кількох осіб тощо.

Незважаючи на те, що підставою внесення законодавчих змін до ст. 335 КПК України було врегулювання питання здійснення кримінальних проваджень в умовах воєнного стану, на жаль, це також стало способом для ухилення окремими особами від потенційної кримінальної відповідальності, оскільки відповідно до ст. 49 КК України призов під час мобілізації не є підставою для зупинення перебігу строків давності. Відтак, у випадку мобілізації обвинуваченого важливим є судовий контроль за проходженням військової служби обвинуваченим щодо якого є зупиненим провадження.

Так, у випадку подання стороною захисту документів про мобілізацію обвинуваченого, суд повинен з'ясувати наступне:

1) куди саме мобілізований обвинувачений (регіон, посада);

2) чи наявна у обвинуваченого можливість брати участь в судових засіданнях в режимі відеоконференції;

3) чи буде в обвинуваченого можливість подавати пояснення щодо доказів у справі (наприклад, якщо кримінальне провадження складається зі 50 томів і обвинувачений не має фізичної можливості мати ці документи із собою).

Вищевказані обставини потрібно аналізувати судом індивідуально щодо кожної особи. Адже, наприклад, навіть мобілізація особи в тиловий підрозділ не свідчить однозначно про можливість такої особи бути присутньою в судовому засіданні, зважаючи на специфіку її діяльності під час проходження військової служби.

Якщо кримінальне провадження здійснюється щодо групи осіб, то у випадку зупинення провадження, суди здійснюють таке з виділенням матеріалів відносно мобілізованого в окреме провадження або без такого виділення.

Зупинивши провадження суди, як правило, періодично скеровують запити до військової частини для підтвердження інформації, чи обвинувачений надалі проходить військову службу, чи не змінились умови проходження такої (можливо, у обвинуваченого з'явилась можливість участі в судових засіданнях). Окрім цього, суди у випадках, коли щодо обвинуваченого невдовзі мають закінчитись строки давності за ст. 49 КК України, поновлюють кримінальні провадження, які були раніше зупинені у зв'язку з мобілізацією обвинуваченого, для того, щоб кримінальне провадження щодо особи було закінчено в межах цих строків. Такі приклади є ***(https://zaxid.net/chi_mozhut_mobilizuvati_zvinuvachenih_u_kriminali_poyasnennya_advokata_olega_mitsika_n1611487). – 2025. – 30.05).***

***

Блог на сайті «Lb.ua»

Про автора: Ярина Ясиневич, громадська активістка, членкиня Ради Коаліції «Реанімаційний пакет реформ»

Покоління на гачку? Як тютюнова індустрія затягує молодь

Станом на 2025 рік кожен другий українець віком 18-29 років вживає тютюнові та нікотинові вироби – порівняно з минулим роком зростання відбулося на 36%. Загалом це не дивно, якщо звернути увагу на агресивне просування тютюновою індустрією новітніх тютюнових та нікотинових виробів та слабке реагування держави, а подеколи – його відсутність. В час глибокої демографічної кризи та виснажливої війни на виживання, така статистика – це катастрофа та пряма загроза державній стійкості та національній безпеці.

Що ж такого робить тютюнова індустрія, що на хвилі популярності здорового способу життя та турботи про себе зростає споживання тютюнових та нікотинових виробів? Як вчать маркетологи, якщо продукт не блищить, його треба гарно "запакувати", продати не сам продукт, а емоцію чи потребу.

Тож давайте розберемо маркетингові гачки, якими тютюнова індустрія чіпляє молодь.

“Менша шкода”

Тютюнові компанії створили тютюнові вироби для електричного нагрівання (ТВЕН, стіки) та просувають їх під соусом меншої шкоди, тоді як більшість досліджень ТВЕНів профінансовані або проведені самою тютюновою індустрією. Завдяки цій омані молодь легше схиляється до початку вживання. 38% молодих споживачів вірять в оманливий міф, що ТВЕНи справді менш шкідливі.

“Та це ж було вже!” – подумають старожили. Так, ідея не нова: колись “менш шкідливими” були тонкі сигарети, сигарети з фільтром, але, як бачимо, історія та медичні діагнози розставили все на свої місця. Так само буде і з ТВЕНами, але ціною здоров’я та життя скількох людей?

В Україні вже є красномовний кейс: нещодавно львівський ресторатор, який перейшов на айкоси (але чомусь вони його не врятували – після трьох років споживання чоловік захворів на рак), виграв справу в Антимонопольному комітеті проти Філіп Морріс. АМКУ визнав, що твердження про меншу шкоду айкос вводять в оману та зобов’язав компанію припинити поширювати подібні твердження.

В свою чергу ВООЗ наголошує, що не існує жодних доказів того, що ТВЕН є менш шкідливими, ніж традиційні тютюнові вироби та наполягає, що будь-які форми вживання тютюну завдають руйнівної шкоди здоров’ю людини, адже містять нікотин, канцерогени та є токсичними.

Вражаючим фактом є те, що значна частина молоді не переходить повністю на нові вироби, а комбінує їх із сигаретами, що лише посилює шкоду. Нині понад 45% людей віком 18–29 років вживають тютюнові або нікотинові вироби, і майже половина з них – кілька різних видів одночасно. Це прямий наслідок агресивного просування “зменшеної шкоди”.

Приємний смак та аромат

Ароматизовані вироби – потужний маркетинговий інструмент залучення нових користувачів. Ягідні, фруктові, м’ятні та десертні смаки маскують гіркоту тютюну, створюючи ілюзію безпечного і приємного досвіду. Це знижує настороженість, полегшує “першу затяжку”, зменшує відчуття подразнення в горлі, що може сприяти частішому та глибшому затягуванню і пришвидшує формування нікотинової залежності. У результаті 81% молодих споживачів ТВЕНів обирають саме ароматизовані варіанти. А понад чверть споживачів цих виробів вказують, що саме привабливі аромати або смаки є головною причиною їх вживання. Усвідомлюючи ризики, 65% дорослих українців підтримують заборону ароматизаторів у таких виробах – громадськість розуміє, що це гачок, а не вибір.

Упаковка – це перший продавець

Пачка сигарет для нагрівання – це не просто обгортка, а потужний маркетинговий інструмент. Її дизайн приваблює молодь і підлітків, формуючи позитивне емоційне ставлення до продукту ще до першої спроби. Через трендові кольори, шрифти та візуальні асоціації тютюнова індустрія просуває залежність як модний стиль. Упаковки виглядають так, ніби це цукерки, жуйки або солодкий снек – усе, тільки не шкідливий виріб. На пачках тютюнових стіків відсутні графічне медичне попередження про наслідки вживання тютюну та інформація про сервіс з надання допомоги у припиненні куріння, які розміщені на сигаретних пачках. Курці ТВЕНів на 20% рідше помічають попередження на пачках, ніж курці сигарет, де такі повідомлення розміщені великим розміром й з картинками хвороб.

Прикметно, що 81% українців підтримує впровадження графічного медичного попередження на пачках ТВЕН та пристроїв. Тому дивує, що парламент досі не відповів на цей високий і консолідований запит виборців.

Тютюнові вітрини – рекламний щит

Яскраві вітрини із ТВЕНами біля кас, трендово оформлені точки продажу – це фактична реклама, яка формує імпульсивне бажання придбати. Колір, підсвітка, оформлення, спеціальні дисплеї, розміщення біля солодощів – усе спрямоване на привернення уваги, особливо дітей та молоді. Усе це створює ілюзію, що куріння – це щось нормальне, соціально прийнятне і модне. Це – точка входу в нікотинову залежність.

За результатами опитування – 75% молоді віком 18-29 років наражаються на рекламу ТВЕН, зокрема більше половини опитаних спостерігали рекламну інформацію, що допомагає просувати ТВЕН, у точках роздрібної торгівлі.

Оманлива, маніпулятивна реклама в інтернеті

Тютюнова реклама в мережі давно вийшла за межі класичних форматів – це "лайфстайл" через інфлюенсерів, жарти, конкурси, візуальні образи свободи. Вона виглядає як розвага, а не як реклама. Попри заборону будь-якої реклами, індустрія успішно обходить обмеження. Вона просуває продукцію через соціальні мережі, банери, відео в Інтернеті, статті у медіа, блогерів, які нативно згадують бренд у своєму контенті, або споживають сигарети для нагрівання під час онлайн-трансляцій, у подкастах тощо. Привабливий стиль, репутація та довіра до інфлюенсерів формують хибне уявлення про "бездимну" альтернативу. Як наслідок, 59% молоді зазначили, що стикаються в інтернеті з просуванням пристроїв для електричного нагрівання та тютюнових стіків.

Водночас, реклама активно спекулює на україноцентричній підтримці та прихильності, використовують українську символіку та патріотичні меседжі. У часи повномасштабної війни, коли є більш лояльне ставлення до всього українського – маскуються під патріотів та спекулюють почуттями суспільства.

Заходи, що просувають культуру куріння ТВЕНів

До повномасштабного вторгнення тютюнові компанії активно спонсорували музичні фестивалі, вечірки, спортивні події, де їхня продукція інтегрувалась через бренд-зони, стенди, подарунки, фотозони.

Після початку великої війни в Україні тютюнові компанії адаптували свої маркетингові стратегії до нових умов, продовжуючи просування своїх продуктів серед молоді. Замість традиційних фестивалів та масових заходів, які стали менш доступними через війну, вони зосередилися на створенні альтернативних соціальних просторів. Наприклад, відкриття просторів «Сфери світла» від IQOS у Києві, Одесі та Львові, оснащених генераторами та Starlink, коворкінг на Хрещатику в Києві, який поєднує функції магазину та простору для роботи й відпочинку, кінозустрічі та читацькі клуби. Ці ініціативи позиціонувалися як соціальна підтримка, але фактично слугують платформами для непрямої реклами та зміцнення лояльності до тютюнових брендів.

"Благодійність"

Чи не найбільш цинічним є те, що тютюнові компанії-спонсори війни розповідають в Україні, які вони благодійники та як підтримують український народ, тоді як на росії платять чи не найбільше податків з усіх міжнародних компаній.

Philip Morris International та Japan Tobacco International у 2023 році отримали найбільшу виручку в росії серед усіх міжнародних компаній – 13,6 млрд дол. та сплатили 402 млн дол. податку на прибуток.

Допомога армії, проєкти для молоді, екологічні ініціативи – усе це відволікає від головного: вони продають залежність. Це ефективна стратегія пом'якшення репутаційних ризиків, яка підриває суспільну настороженість.

Законопроєкт №12091: важливий крок для захисту молоді

Щороку понад 100 тисяч українців помирають від хвороб, спричинених курінням – і в умовах демографічної кризи це вже не лише питання здоров'я, а й національної безпеки. Держава має зупинити цю хвилю залежності. І є чітке рішення, яке підтримують самі українці.

У Верховній Раді з жовтня минулого року лежить законопроєкт №12091, спрямований ліквідувати маркетингові заходи тютюнової індустрії та захистити дітей та молодь від втягування у залежність. Окрім того законопроєкт є євроінтеграційним – імплементує положення Директиви 2014/40/ЄС. Документ передбачає:

запровадження обов'язкових попереджень на пачках ТВЕН;

заборону смакових добавок;

заборону тютюнової викладки;

посилення контролю за онлайн-просуванням;

підвищення акцизів.

Авторами законопроєкту є народні депутати з різних фракцій та груп – зокрема, представники

фракцій «Слуга народу», «Європейська солідарність», «Голос» та депутатських об'єднань. Це свідчить про широку міжфракційну підтримку ініціативи, яка має на меті захистити молодь від втягування у нікотинову залежність.

Ми очікуємо, що найближчим часом Комітет з питань здоров'я нації розгляне законопроєкт та винесе на розгляд парламенту. Це тест на відповідальність – за здоров'я, за майбутнє нашої молоді, за європейський курс держави.

В умовах повномасштабної війни та глибокої демографічної кризи кожне життя – на вагу золота. Ми не можемо дозволити собі щороку втрачати 100 000 українців через хвороби, спричинені тютюном. Особливо – молодь, від якої залежить економічна стійкість, обороноздатність та саме існування української держави ***(https://lb.ua/blog/yaryna_yasynevych/679263_pokolinnya_gachku_yak_tyutyunova.html). – 2025. – 30.05).***

ГРОМАДСЬКА ДУМКА ПРО ПРАВОТВОРЕННЯ

№ 10 (296) 2025
Інформаційно-аналітичний бюлетень
на базі оперативних матеріалів
Додаток до журналу «Україна: події, факти, коментарі»
Ідентифікатор медіа R30-01101

Редактори:
А. Берегельська, Я. Маленко

Комп'ютерна верстка:
Н. Крапіва

Підп. до друку 26.05.2025
Формат 60х90/8. Обл.-вид. арк. 3,67.
Наклад 21 пр.

Видавець і виготовлювач
Національна бібліотека України
імені В. І. Вернадського
03039, м. Київ, Голосіївський просп., 3
siaz2014@ukr.net
Свідоцтво про внесення суб'єкта
видавничої справи до Державного реєстру видавців,
виготовлювачів і розповсюджувачів
видавничої продукції ДК № 7871 від 28.06.2023 р.