



# **СТРАТЕГІЯ 2020**

**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ  
В ДЕРЖАВНОМУ УПРАВЛІННІ**

НАЦІОНАЛЬНА БІБЛІОТЕКА УКРАЇНИ ІМЕНІ В.І. ВЕРНАДСЬКОГО  
ФОНД ПРЕЗИДЕНТІВ УКРАЇНИ

**«Інформаційні технології в державному  
управлінні»  
Ініціативи Президента України**

---

**Інформаційно–бібліографічний бюлетень**

**Головний редактор**

С. В. Полтавець, в.о.директора Фонду Президентів України,  
канд. політ. наук, ст. наук. співроб.

**Відповідальні за випуск**

В.М. Удовик, ст. наук. співроб. інформаційно–аналітичного відділу  
Фонду Президентів України, канд. іст. наук

**Інформаційні та бібліографічні матеріали підготували**

В.М. Удовик, Л.Г. Дем'яненко,  
М.Б. Кушнар'ова, Є.В. Глушук

Заснований у 2014 році  
Виходить один раз на місяць

**Адреса редакції:**

НБУВ, пр–т Голосіївський, 3, Київ, 03039, Україна  
Тел. (044) 525–54–70  
E–mail: [fpu@nbuv.org.ua](mailto:fpu@nbuv.org.ua)

Передрук – тільки з дозволу редакції

© Національна бібліотека України  
імені В. І. Вернадського, 2020

Передрук за погодженням

# **«Інформаційні технології в державному управлінні»**

**(Ініціативи Президента України)**

**Випуск 11 (85)**

*(огляд матеріалів ЗМІ за 1 – 30 листопада 2020 р.)*

## **Зміст**

<b>Анонс.....</b>	<b>4</b>
<b>Офіційна інформація.....</b>	<b>5</b>
<b>Регіональні ініціативи.....</b>	<b>15</b>
<b>Експертний погляд.....</b>	<b>17</b>
<b>Блоги та соціальні мережі .....</b>	<b>23</b>
<b>Зарубіжний досвід.....</b>	<b>42</b>
<b>Новітня бібліографія зарубіжних та вітчизняних досліджень з проблематики електронного урядування.....</b>	<b>59</b>

## **Анонс**

09–11 грудня 2020 р. (Київ)

**Фестиваль «Цифрова трансформація: молодь за краще майбутнє».**

*Початок:* 09.12.2020 о 15:00

*Закінчення:* 11.12.2020 о 18:00

*Місце:* онлайн, Платформа ZOOM, Інститут Регіонального Розвитку

Цифрова трансформація дає поштовх до розвитку політичної активності молоді. Інструменти електронної демократії підвищують участь громадян у процесі прийняття рішень. Криза COVID-19 показала, що цифрові технології мають важливе значення для нашої економіки та повсякденного життя. Люди зробили великий «цифровий стрибок» під час цієї кризи, перемістивши свою роботу, навчання та соціальне життя в Інтернет. Але локдаун також виявив прогалини в нашій цифровій інфраструктурі.

***Наше прагнення:*** посилити участь громадян і, зокрема молоді, в житті країни, проведенні позитивних перетворень завдяки цифровій трансформації.

***Для кого:*** організації громадянського суспільства, молоді активісти, експерти з цифрової трансформації та інформаційних технологій, соціально-активний бізнес, представники органів влади

Захід проводиться в рамках проекту «Hackyourfuture», що реалізовується GlobalProjectPartners.V. ([www.global-project-partners.de](http://www.global-project-partners.de)) спільно з Інститутом Регіонального Розвитку (<https://www.institute.lviv.ua>) за фінансової підтримки Федерального Міністерства Закордонних Справ Німеччини (<https://www.prostir.ua/event/festyval-tsyfrova-transformatsiya-molod-za-krasche-majbutnje/>).

## **Офіційна інформація**

**Мінцифри проведе багбаунті мобільного застосунку Дія з призовим фондом 1 млн грн. У грудні буде відкрито прийом заявок для «білих хакерів».**

Мінцифри постійно працює над посиленням безпеки мобільного застосунку Дія. Адже для нас надзвичайно важливо, щоб користувачі були впевнені у захищеності їх персональних даних.

На Дію 2.0 отримано атестат КСЗІ – мобільний застосунок відповідає українським стандартам. Дія успішно пройшла 2 пентести за підтримки проекту USAID «Кібербезпека критично важливої інфраструктури в Україні» та Академії електронного урядування Естонії.

Тепер Мінцифри дає можливість «білим хакерам» протестувати захищеність мобільного застосунку Дія. Зараз ми фіналізуємо деталі щодо правил багбаунті, умов участі та класифікації типів вразливостей по категоріях. У грудні буде відкрито прийом заявок.

**Умови проті:** за кожен знайдений недолік системи (баг) – хакер отримує винагороду.

Призовий фонд – 1 млн грн (\$35 тисяч). Нагороди будуть розподілені за категоріями складності знайдених багів.

Важливо, що під час багбаунті, хакери намагатимуться зламати «тестовий застосунок». Буде створено окреме середовище для пошуку багів, яке не буде містити персональні дані.

Багбаунті реалізується за підтримки проекту USAID «Кібербезпека критично важливої інфраструктури в Україні» (*Мінцифри проведе багбаунті мобільного застосунку Дія з призовим фондом 1 млн грн. // <https://www.kmu.gov.ua/news/mincifri-provede-bagbaunti-mobilnogo-zastosunku-diya-z-prizovim-fondom-1-mln-grn>. – 2020. – 27.11*).

**Рейтинг електронної участі ООН формується в рамках дослідження UN E-government Survey.**

Про це повідомила **заступниця Міністра цифрової трансформації Людмила Рабчинська** на Ukraine Reform Conference – міжнародній події, присвяченій експертному обговоренню прогресу реформ в Україні.

«Сьогодні Україна посідає 46 місце зі 193 країн світу – учасниць рейтингу. Вже у 2022 році ми прагнемо увійти до ТОП-20 країн рейтингу. Лідерами цього рейтингу є Естонія, Південна Корея, США, Японія та Нова Зеландія»...

Зокрема, **для цього Міністерство цифрової трансформації:**

Готує до запуску онлайн-платформу «ВзаємоДія» за підтримки Програми EGAP, що реалізується Фондом Східна Європа. Завдяки цьому громадяни отримають доступ до таких сервісів, як: е-звернення та запити на публічну інформацію, е-консультації з громадськістю, е-петиції до Кабміну, е-конкурси проєктів та програм інститутів громадянського суспільства, е-

вибори членів громадських рад при органах виконавчої влади, а також конкурси проектів Всеукраїнського громадського бюджету. Перші сервіси очікуються до кінця 2020 року.

*Підтримує ініціативу Президента України Володимира Зеленського щодо запровадження інтернет-голосування на виборах та референдумі.* Зокрема, і-voting на президентських виборах 2024 року. Саме для цього ми досліджуємо кращі практики і-voting та готуємось до співпраці з ключовими стейкхолдерами – органами державної влади, щоб стати драйвером процесу запровадження інтернет-виборів в Україні із забезпеченням кібербезпеки та з побудовою довіри громадян до таких виборів. Окрім цього, триває робота над розробкою нормативної бази для розвитку прямої демократії в Україні та надаються пропозиції щодо цифровізації процесу референдуму, а саме е-збору підписів та е-голосування.

*Формує Концепцію цифрової трансформації громад.* Це допоможе визначити проблематику розвитку е-демократії на місцевому рівні та запропонувати план заходів стосовно її вирішення.

*Підтримує та надає свої пропозиції до законопроекту «Про публічні консультації»,* розробленого Мін'юстом. Це дозволить представникам органів влади проводити е-консультації централізовано, відповідно до кращих світових практик, а також продемонструє реальний зв'язок між ухваленими рішенням та результатами публічних консультацій.

За ініціативи Мінцифри Державна служба статистики та Центр розвитку інновацій проводять статистичні спостереження й дослідження. Це дозволить глибше зрозуміти проблематику громад та органів державної влади і місцевого самоврядування у сфері е-демократії. А також допоможе запропонувати план дій на загальнодержавному та регіональному рівнях (*Мінцифра: Україна піднялася на 29 позицій у рейтингу індексу електронної участі ООН // <https://thedigital.gov.ua/news/mintsifra-ukraina-pidnyalasya-na-29-pozitsiy-u-reytingu-indeksu-elektronnoi-uchasti-oon>. – 2020. – 26.11).*

Українці зможуть здійснювати касові операції у банках із цифровими паспортами у Дії з 1 грудня. Таку можливість затвердив Національний банк у роз'яснювальному листі на своєму сайті.

«Банківські послуги стають ще зручнішими. Національний банк опублікував роз'яснювальний лист на сайті, що з 1 грудня завдяки електронним паспортам у Дії можна верифікувати та ідентифікувати свою особу для здійснення касових операцій у банку», – прокоментував **віцепрем'єр-міністр – Міністр цифрової трансформації Михайло Федоров**.

Команда Мінцифри однією з перших у світі запустила послугу шерингу цифрових документів. Відтепер клієнтам банків, які мають електронний паспорт у застосунку Дія, більше не потрібні паперові документи для підтвердження своєї особистості в банківському відділенні. Мінцифра навчає

банки оптимізувати процеси з допомогою шерингу документів, а не паперових носіїв, як раніше (паспортів, копій документів тощо).

Тепер громадянам будуть доступні верифікація та ідентифікація особи з електронним паспортом для здійснення касових операцій у банку. Для цього можна використовувати як ID-картку, так і закордонний біометричний паспорт громадянина у мобільному застосунку Дія. Це значно спростить проведення касових операцій банками під час обслуговування клієнтів.

Відповідні норми містить постанова Правління Національного банку України від 23 листопада 2020 року № 148 «Про затвердження Змін до Інструкції про ведення касових операцій банками в Україні», що набирає чинності з 1 грудня 2020 року.

Мінцифра спільно із Нацбанком активно цифровізує банківську сферу. З жовтня у всіх відділеннях ПриватБанку та А-Банку можна скористатися шерингом документів. А в Монобанку можна відкрити рахунок повністю онлайн із документами в Дії (*Михайло Федоров: «З грудня українці зможуть здійснювати касові операції в банках з е-паспортом в Дії» // <https://thedigital.gov.ua/news/mihajlo-fedorov-z-grudnya-ukrayinci-zmozhut-zdijsnyuvati-kasovi-operaciyi-v-bankah-z-e-pasportom-v-diyi>. – 2020. – 26.11).*

**9,6 млн євро – перший фінансовий внесок, який отримає Україна у рамках проекту EU4DigitalUA.** Він спрямований зробити урядову цифрову інфраструктуру функціональною і надасть підтримку в побудові надійної системи електронних послуг.

Естонська Академія електронного урядування (e-Governance Academy) керуватиме процесом імплементації та досягнення цілей.

***Мінцифра з європейськими партнерами окреслила майбутні плани:***

- розробка інфраструктури для цифрового врядування
- модернізація державних електронних послуг
- розвиток кібернетичної безпеки і засобів захисту даних
- візуалізація інформації щодо доступу до широкопasmового інтернету в Україні
- продовження підключення основних реєстрів до системи обміну даними «Трембіта»
- розробка загальнодержавного персонального ідентифікатора – державного цифрового посвідчення особи і реєстру адрес реєстрації місця проживання громадян
- розробка електронних послуг на порталі Дія та в застосунку Дія
- смарт-Дія та розвиток довірчих послуг
- бродбенд платформа.

«Ми вдячні ЄС за підтримку цифрової трансформації України. Вже понад рік команда Мінцифри будує цифрову державу. Цифрова трансформація є ключем до реформи будь-якої сфери. Ми вже це продемонстрували на прикладі галузі містобудування та адміністративних

послуг. Підтримка цифрової трансформації в Україні – це одночасно підтримка всіх ключових реформ і антикорупційної діяльності. Ми готові обмінюватись досвідом з іншими країнами та щодня вдосконалювати проекти, над якими працюємо. Завдяки допомозі ЄС Україна отримає більше якісних змін», – заявив **віце-прем'єр-міністр – Міністр цифрової трансформації України Михайло Федоров**.

Представники ЄС наголосили: Україна досягла вражаючих успіхів у цифровій трансформації – посіла 69-е місце у рейтингу ООН серед 193 країн щодо готовності до електронного Уряду за індексом EDGI. Україна піднялася на 16 позицій у порівнянні з 2018 роком.

«ЄС підтримує подальший розвиток цифрових технологій в Україні з метою підвищення конкурентоздатності країни і сприяння подальшому наближенню України до Єдиного цифрового ринку ЄС», – зауважив під час установчого засідання проекту **Голова Представництва ЄС в Україні Посол Матті Маасікас**.

Мінцифра вже має успішний цифровий досвід співпраці з європейськими партнерами. Естонська Академія електронного управління ще з 2012 року здійснює реалізацію проектів з електронного врядування в Україні. Завершується проект eGov4Ukraine, результатом якого є успішне запровадження системи «Трембіта» та «Вулику». Трембіта вже стала основою реєстрів країни. Лише за цей рік ми маємо понад 5 млн транзакцій – обмінів через систему.

«Ми застосовуємо передовий досвід, отриманий при розбудові «цифрового уряду» Естонії, щоб допомогти Україні в подальших кроках до створення більш прозорого і ефективного суспільства», – наголосив **Ханнес Асток, Виконавчий директор Академії електронного управління**.

Проект EU4DigitalUA – це частина широкої підтримки Європейським Союзом розвитку електронного врядування в Україні. Реалізацію втілюватимуть Іспанська фундація FIPAPP Spain та естонська Академія електронного управління. Європейський Союз продовжує підтримувати цифрову трансформацію України та її гармонізацію з Єдиним цифровим ринком *(ЄС надасть Україні 25 млн євро фінансової підтримки на розвиток цифрової трансформації, якою займається Мінцифра // <https://www.kmu.gov.ua/news/yes-nadast-ukrayini-25-mln-yevro-finansovoyi-pidtrimki-na-rozvitok-cifrovoyi-transformaciyi-yakoyu-zajmayetsya-mincifra>. – 2020. – 25.11)*.

Запуск е-лікарняних дозволить не лише скасувати лікарняний як паперову довідку, що є елементом бюрократії, а й заощаджувати час лікарів та пацієнтів. Крім цього, це можливість швидко та ефективно оплачувати лікарняні без фізичних контактів, гарантувати обґрунтованість виплат та економити державні кошти.

Про це розповів **віцепрем'єр-міністр – Міністр цифрової трансформації Михайло Федоров** в ефірі каналу 24.



Однією з можливих проблем запровадження е-лікарняних називають необхідність дублювати документи у цифровому та паперовому вигляді.

«Це не так: електронні лікарняні будуть одразу в електронному вигляді, нічого дублювати не потрібно. Це буде звичайна форма в онлайн-системі, заповнення якої займатиме кілька хвилин. Після цього підписаний електронним підписом документ автоматично надсилатиметься до інших державних органів для виплат».

Для запровадження електронних лікарняних Міністерство цифрової трансформації спільно з Міністерством охорони здоров'я повністю перебудовують процес отримання лікарняного. Запуск стане можливим завдяки повноцінній інтеграції електронної системи охорони здоров'я із системою Пенсійного фонду України і Фонду соціального страхування України

Для того, щоб революційні медичні послуги стали доступними для всіх українців, Міністерство цифрової трансформації активно працює над підключенням до інтернету 95 % населених пунктів та їхніх соціальних об'єктів.

Наразі, до оптичного (фіксованого) інтернету не підключено 37 % лікарень України. У 2021 році Мінцифра планує підключити близько 10 тисяч соціальних об'єктів: шкіл, лікарень, бібліотек, які знаходяться у 5 тис. сіл, де проживають майже 2,5 млн громадян.

На минулому тижні, Кабінет Міністрів України підтримав пропозицію Мінцифри – закласти у бюджет на 2021 рік 850 млн гривень на підключення соціальних об'єктів до високошвидкісного інтернету у населених пунктах, в тому числі у сільській місцевості (*Михайло Федоров: Запустимо е-лікарняні вже з 2021 року // <https://thedigital.gov.ua/news/mikhaylo-fedorov-zapustimo-e-likarnyani-vzhe-z-2021-roku>. – 2020. – 24.11).*

**Міністерство цифрової трансформації разом із проєктом USAID/UK aid «Прозорість та підзвітність у державному управлінні та послугах/TAPAS» презентували результати якісного дослідження про вплив відкритих даних у сфері будівництва, реконструкції, ремонту та утримання автомобільних доріг в Україні.** У ньому проаналізували, як оприлюднення даних впливає на життя громадян, провадження бізнесу та діяльність органів влади, а саме: які дані дають змогу моніторити витрати у дорожній сфері та виявляти порушення під час закупівель, де шукати ці дані, за допомогою яких інструментів громадяни можуть скаржитися на проблеми з дорогами у своїх населених пунктах і змушувати владу усувати їх.

Ще кілька років тому було неможливо зрозуміти та відстежити, як витрачають державні кошти на ремонти та утримання доріг в Україні. Сьогодні ж громадськість має доступ до сотень тисяч договорів публічних закупівель у дорожній галузі, що містяться у системі Prozorro. А на Єдиному державному вебпорталі відкритих даних Укравтодор і служби автомобільних

доріг оприлюднюють дані про фінансування дорожньої галузі, про виконання планових та поточних ремонтів тощо.

*Попри відкритість інформації, існує низка потенційних корупційних ризиків.* У 2019 році правоохоронні органи визначили, що корупційна складова від загальної вартості ремонту та утримання доріг становить 10–15 %. Це може бути близько 10-15 млрд гривень із розрахунку, що у 2020 році на цю сферу в Україні передбачено фінансування близько 100 млрд гривень.

У дослідженні описують, який вплив має відкриття даних про ремонти доріг в Україні та які можливості воно створює для вирішення проблемних питань дорожньої галузі. **Серед усього:**

*Виявляти змови виконавців.* Інструменти на основі відкритих даних та аналіз документів із системи Prozorro допомагають відслідкувати поведінку учасників на тендерах, зв'язки між компаніями, де і як вони отримують довідки та готують документи для подання на тендер тощо.

*Знаходити порушення під час тендерів з боку замовників.* Схеми, коли дорогу ділили на шматки, щоб уникнути проведення тендеру, застосування нецінових критеріїв і прописування дискримінаційних вимог під певних виконавців – усе це можна виявити завдяки інформації, що міститься у Prozorro, і таким чином сприяти скасуванню проблемних закупівель послуг.

*Удосконалювати процедуру закупівель.* Аналіз тендерних заявок, рекомендацій та інших документів автодорожніх структур дає змогу виявити порушення у процедурах закупівель та усувати недоліки на законодавчому рівні.

*Подавати скарги на поганий ремонт доріг.* Завдяки таким громадським сервісам на основі відкритих даних, як «Прозора інфраструктура» та «Антикорупційна карта ремонтів», мешканці можуть перевірити стан і якість відремонтованої дороги та повідомити про наявні недоліки для їх усунення.

*Контролювати ефективно використання бюджетних коштів.* Використовуючи дані на порталах data.gov.ua та spending.gov.ua, громадськість може перевірити невикористані кошти на утримання доріг та змушувати владу проводити ремонт.

*Перевіряти підрядників.* За допомогою сервісу «Прозора інфраструктура» замовники можуть оцінити досвід виконавців та якість попередніх робіт.

*Перевіряти фахівців дорожніх структур на належне виконання обов'язків.* Аналіз договорів з інженерами технічного нагляду за ремонтом доріг, обсягу їх навантаження та звітів технагляду дає змогу виявити недобросовісне надання послуг та корупційні схеми.

Більше прикладів використання відкритих даних у дорожній сфері можна знайти у звіті за посиланням: <http://tapas.org.ua/wp-content/uploads/2020/11/Open-data-impact-road-sector.pdf>.

Цей звіт є другим із серії якісних досліджень, в яких аналізують вплив відкриття даних на галузі економіки України. У вересні презентували перше дослідження про відкриті дані Державної архітектурно-будівельної

інспекції України *(В Україні проаналізували, як відкриті дані впливають на ремонт і будівництво доріг // <https://newskm.net/news/v-ukraini-proanalizuvaly-iak-vidkryti-dani-vplyvaiut-na-remont-i-budivnytstvo-dorih>. – 2020. – 18.11).*

**Уряд презентував Економічний аудит країни Re:Think та окреслив основні вектори розвитку української економіки.**

Результати аудиту ляжуть в основу Національної економічної стратегії до 2030. Мінцифра готує проекти для залучення інвестицій в Україну.

«Документ Re:Think – це переосмислення економічного потенціалу нашої держави. Уперше було зроблено комплексний аналіз стану країни, щоб зрозуміти – де саме та які саме були допущені помилки за ці роки», – наголосив **Прем'єр-міністр України Денис Шмигаль**.

Робота у 30 пріоритетних напрямках дозволить отримати 1 трлн доларів ВВП за 10 років. Стільки, за підрахунками, становить нереалізований потенціал країни через постійні зміни векторів, незавершені реформи та відсутність довгострокової економічної стратегії.

*До переліку основних векторів розвитку економіки України потрапили проекти*, що реалізуються спільно з Міністерством цифрової трансформації. Команда Мінцифри готує проекти Дія City та e-Резидентство, що сприятимуть збільшенню інвестиційної привабливості України, покращенню бізнес-клімату, розвитку інформаційно-комунікаційних технологій та цифрової економіки.

Загальний інвестиційний потенціал України оцінюється у 63 млрд доларів. Для залучення іноземних інвестицій, держава працюватиме над створенням привабливих правових та податкових умов для ІТ-компаній. Для цього Мінцифра створила проєкт Дія.City – цифрової бізнес-країни зі спеціальним правовим режимом для ІТ-індустрії. За підрахунками, запуск Дія. City може збільшити об'єм ринку ІТ до \$11,8 млрд вже за 5 років.

Запорукою розвитку цифрової економіки визначили всебічну цифрову трансформацію країни. Серед головних цілей візії – удосконалення цифрової інфраструктури, забезпечення 95 % населення доступом до високошвидкісного інтернету, створення комфортних умов для ведення бізнесу в Україні, цифровізація державних послуг, підвищення базової цифрової грамотності населення, інтеграція до цифрового простору ЄС тощо. Цифровізація усіх сфер здатна у найкоротший час «розігріти» українську економіку й забезпечити її зростання на 10–12 % на рік *(Цифровізація – один з головних векторів розвитку економіки у наступні 10 років // <https://thedigital.gov.ua/news/tsifrovizatsiya-odin-z-golovnikh-vektoriv-rozvitku-ekonomiki-u-nastupni-10-rokiv>. – 2020. – 07.11).*

**Державною податковою службою України запроваджено електронний сервіс «InfoTAX».**

Через месенджери Telegram та Viber платники податків мають можливість отримувати інформацію про:

- стан розрахунків з бюджетом,
- реєстраційні та облікові дані,
- про результати обробки документів,
- про строки подання звітності та сплати податків.

Для покращення роботи електронного сервісу пропозиції та зауваження до нього просимо надсилати на адресу [infozvit@tax.gov.ua](mailto:infozvit@tax.gov.ua).

Наступний етап сервісу буде запроваджено з січня 2021 року та надаватиме такі можливості:

- передзаповнення звітності для платників єдиного податку,
- перехід до сплати податків у «два кліки»,
- оповіщення про виникнення податкового боргу, а також про можливість виникнення податкового боргу у разі несвоєчасної сплати.

Для доступу до сервісу необхідно у відповідному месенджері (наприклад, Telegram) знайти InfoTAX, в якому перейти за посиланням до Електронного кабінету для ідентифікації та завершення налаштування нового сервісу.

«InfoTAX» – це продовження розпочатого ДПС курсу на максимально дистанційне спілкування з платниками податків та якісно новий рівень послуг. Комфортність спілкування з податковою службою, швидкість та зручність отримання податкової інформації через «InfoTAX» є не просто черговим кроком ДПС у напрямі цифровізації, а відповіддю на запит платників у мобільності отримання послуг (*Розпочав роботу електронний сервіс «InfoTAX» // <https://www.kmu.gov.ua/news/rozpochav-robotu-elektronnij-servis-infotax>. – 2020. – 06.11*).

**Google Україна за активної підтримки МОН організовує безоплатне навчання для педагогічних працівників закладів загальної середньої освіти за курсом «Ефективні рішення Google for Education для хмарної взаємодії».** Навчання триватиме з 12 до 22 листопада 2020 року.

«Надання нашим вчителям можливостей опанувати навички з організації дистанційного навчання з використанням сучасних цифрових інструментів є сьогодні одним із наших ключових пріоритетів. І ми дуже вдячні представникам ІТ-спільноти за активну співпрацю у цьому напрямі», – зазначив **заступник Міністра освіти і науки України Артур Селецький**.

***Під час навчання учасники опрацюватимуть матеріали з таких практичних напрямів:***

- можливості додатків Google Workspace (G Suite) при роботі з вебінтерфейсом персональних комп'ютерів;
- використання додатків Google Workspace (G Suite) на мобільних пристроях;
- опрацювання основних налаштувань безпечної роботи в Інтернеті.

Програма курсу розрахована на 15 годин і складається із таких змістових частин:

5 модулів, які складаються з 2-х годин відеолекцій (можна переглядати в записі) разом з тренером;

1 година на самостійне опрацювання;

1 година – складання підсумкового тесту.

Під час навчання вчителі забезпечуватимуться методичним супроводом та консультаціями, на період навчання їм буде наданий доступ до тимчасового персонального облікового запису в реальній системі для ознайомлення з системою G Suite for Education.

Ефективний зворотній зв'язок із учасниками курсу налаштований через системи сповіщень, здачі робіт, отримання приватних консультацій до кожного завдання в середовищі Google Класу. Окремо буде забезпечено можливість вчителям отримати консультації через спеціально організовані зустрічі з тренерами в Google Meet.

За умови успішного проходження навчання (виконання 80 % усіх запропонованих завдань та 80 % правильних відповідей на запитання підсумкового тесту) учасники отримають електронний сертифікат про проходження курсу, який може бути зарахований як підвищення кваліфікації *(МОН та Google Україна ініціюють безкоштовне навчання для вчителів з використання цифрових інструментів для дистанційного навчання // <https://www.kmu.gov.ua/news/mon-ta-google-ukrayina-iniciyuyut-bezkoshtovne-navchannya-dlya-vchiteliv-z-vikoristannya-cifrovih-instrumentiv-dlya-distancijnogo-navchannya>. – 2020. – 06.11).*

**Відтепер органи влади, замовники і постачальники можуть надсилати офіційні листи до державного підприємства «Прозорро» через систему електронного документообігу.**

Як передає Укрінформ, про це повідомляється на сторінці Прозорро в Фейсбук.

«Більше не потрібно купувати папір, друкувати лист на принтері, облизувати конверт та чекати поки лист прийде поштою. Краще – скористатися системою електронного документообігу Prozorro», – йдеться в повідомленні.

Прозорро також створило інструкцію, як подати офіційний лист за допомогою системи електронного документообігу.

Для цього потрібно увійдіть в систему за допомогою КЕП, Mobile ID або створивши обліковий запис організації; створити угоду і надати доступ до неї контрагенту – ДП «Прозорро»; завантажити документ до угоди і накласти свій кваліфікований електронний підпис.

Відповідь від Прозорро надійде електронною поштою, за якою той, хто звертався, зареєстрував свою організацію. Прочитати відповідь також можна буде в системі ЕДО, перейшовши за наданим посиланням *(Прозорро запустило систему електронного документообігу //*

<https://www.ukrinform.ua/rubric-economy/3130464-prozorro-zapustilo-sistemu-elektronnogo-dokumentoobigu.html>. – 2020. – 05.11).

**Вже протягом двох років, з моменту набуття чинності Законом України «Про електронні довірчі послуги», українці отримують лише сучасні електронні підписи європейського типу – кваліфіковані та удосконалені.**

Таким чином Мінцифри разом іншими державними органами забезпечили українцям можливість без перешкод перейти на нові електронні підписи та зручно ними користуватися.

«За півроку близько 4,5 млн разів користувачі перевірили та наклали електронний підпис на сервісах Мінцифри. Для нас важливо, щоб електронні довірчі послуги були доступними, безпечними та сучасними для всіх українців,» – підкреслює **заступник Міністра цифрової трансформації з розвитку публічних послуг Людмила Рабчинська**.

***Які можливості є наразі в користувачів електронних довірчих послуг?***

Удосконалений електронний підпис призначений для масового використання. Він найбільш доступний і за останні два роки прийшов на заміну застарілого ЕЦП. 92 % громадян користуються саме таким підписом. Головна його особливість – можливість зберігання на файловому носії, наприклад звичайній флешці. Використовується у більшості життєвих ситуацій. Зокрема, під час отримання е-послуг на порталі Дія, наприклад, при відкритті ФОП.

Кваліфікований електронний підпис призначений для використання в ситуаціях, які потребують підвищеного захисту. Наприклад, державними службовцями чи нотаріусами. Головна його відмінність від удосконаленого електронного підпису – зберігання на захищеному носії – токени чи у хмарі.

Протягом двох років відбувався перехід на нові електронні підписи. За цей період закінчилася дія усіх ЕЦП, адже термін їх використання саме два роки. Отже, усі електронні підписи, які видані протягом дії закону, дійсні.

Важливо: отримати кваліфіковані та удосконалені електронні підписи можна у кваліфікованих надавачів електронних довірчих послуг. Їх перелік за посиланням: <https://czo.gov.ua/ca-registry> (Мінцифри: ***Усі електронні підписи, які мають українці, дійсні*** // <https://www.kmu.gov.ua/news/mincifri-usi-elektronnii-pidpisi-yaki-mayut-ukrayinci-dijsni>. – 2020. – 04.11).

## **Регіональні ініціативи**

**Міністерство цифрової трансформації завдяки проєкту Дія.Цифрова освіта отримало можливість комп'ютеризувати міста та села і передати за сприяння Української бібліотечної асоціації комп'ютерну техніку сільським бібліотекам Львівщини.**

**Заступник Міністра цифрової трансформації з питань євроінтеграції Валерія Іонан** підкреслила, що у невеликих містах і селах бібліотеки є особливо важливими локаціями для місцевих мешканців.

«Наша задача – за допомогою комп'ютеризації перетворити бібліотеки на сучасні багатофункціональні простори, як у розвинутих країнах. Забезпечення технікою і доступ до Інтернету – це базові речі для бібліотек у XXI столітті, які дозволяють їм перетворитися на хаби цифрової освіти. Наша масштабна ініціатива допоможе сільським бібліотекам стати ще більш привабливими і корисними для жителів», – заявила Валерія Іонан.

**Генеральний директор директорату внутрішньої та гуманітарної політики Офісу Президента Вероніка Селега** наголосила на необхідності об'єднання зусиль приватного сектору, органів державної влади та місцевої влади для комп'ютеризації міст і сіл України.

**Заступник голови Львівської ОДА Іван Собко:**

«Ми вже давно перестали асоціювати міські бібліотеки лише з книгозбірнями. Адже це осередки інтелектуального та культурного життя, дозвілля й розвитку наших дітей. І дуже тішить, що сьогодні, завдяки проєкту «Дія.Цифрова освіта» і сільські бібліотеки мають можливість стати платформою для якісної цифрової освіти».

На реалізацію проєкту не витрачені кошти державного бюджету. Це стало можливим завдяки передачі техніки партнерами – Favorit Foundation.

**Маріанна Ковеня, куратор проєктів БФ Favorit Foundation** запевнила, що фонд і надалі підтримуватиме національні проєкти з цифрової освіти. Розвиток інноваційної інфраструктури для освіти та культури пріоритетний напрямок для фонду.

**Голова правління Асоціації розвитку туризму Фазиль Аскеров** заявив, що передача комп'ютерів до сільських бібліотек матиме позитивні соціально-економічний і культурний ефекти.

**Президент ГО «ВГО Українська бібліотечна асоціація» Оксана Бруй:**

«Я переконана, що саме бібліотеки можуть стати тим драйвером, який змінить ситуацію із цифровою грамотністю в Україні із мінуса в плюс. А наявність комп'ютерів та доступу до інтернет у бібліотеках змінить самі бібліотеки та дасть їм відповідні спроможності» *(Мінцифра з партнерами комп'ютеризувала бібліотеки Львівщини //*

---

***<https://thedigital.gov.ua/news/mintsifra-z-partnerami-kompyuterizuvala-biblioteki-lvivshchini>. – 2020. – 19.11).***



## **Експертний погляд**

Нещодавно eZdorovya випала нагода поспілкуватися з командою **Марта БОТ**, серед її очільників: **Дмитро Сергєєв – CEO Open Data Lab – Ukraine, Вікторія Євдокімова – фахівчиня з комунікацій проєкту «Медбот Марта», головний спеціаліст Департаменту охорони здоров'я Маріупольської міської ради, Сергій Сергєєв- Керівник проєкту «Медбот Марта».**

Дмитро: Доброго дня. Ми – команда, що створили Марта БОТ (<https://martabot.pro>). Наша команда розпочала працювати над проєктом ще 20 травня 2018 го року. Через назву місяця російською, так і назвали: «бот Марта».

*Основними напрямками нашої діяльності є Smart-city та eHealth.* Один з вдалих наших кейсів – медичний портал міста Маріуполь, де вже є змога слідкувати за медичною інфраструктурою міста. Наразі ним користуються понад 135 000 мешканців на місяць. Ще один вдалий проєкт – Медбот Марта, яка доповнює наданий спектр послуг і стрімко розвивається не лише в Маріуполі, а й в інших містах України. Також займаємось впровадженням МІС у всіх медзакладах Маріуполя.

*- Як у Вас виникла ідея створення боту?*

Вікторія: В березні 2018-го року ми запустили новий канал комунікації, який дозволяє інформувати пацієнтів про можливості медреформи. Був саме початковий період її трансформації і в усіх виникало безліч питань про декларації, сімейного лікаря, первинну допомогу, тощо. І Марта допомогла відповісти на стандартні питання та знизити кількість частих запитань до медичного персоналу. Це був перший етап впровадження Марти, далі відбувся ребрендинг, де ми оновили інформацію про Марту, розширили список запитань та додали вакцинацію. Також суттєво розширили сам функціонал – тепер комунікувати можна не лише через Facebook, а й через інші месенджери (Viber, Telegram). Щодня Марта стає більш популярною в багатьох містах України.

Зараз дуже важливо займатись медичними сервісами, а не тільки медичними послугами, щоб медичний заклад теж отримував зворотній зв'язок безпосередньо від пацієнтів.

*- Що надихнуло Вас на створення боту?*

Вікторія: Закоханість у медичну галузь загалом. Та, безсумнівно, потреба в популяризації реформи первинної ланки. Щоб передбачити питання: «А що буде далі?» та інформувати про нові впровадження. Ми ефективно розвиваємо медпортал Маріуполя і отримуємо велику кількість однотипних питань, які вирішувались в зручному та доступному форматі за допомогою створення боту.

Ми допомогли багатьом користувачам знайти своїх лікарів та зрозуміти переваги медреформи для кожного.

*- В чому ключове завдання вашої розробки? Розкажіть, будь ласка, про ідею та використання.*

Сергій: В Марті ми створили зручну взаємодію між пацієнтом та медзакладом. В роботі використовуємо державні реєстри відкритих даних. Наприклад, реєстр НСЗУ. Ми є одним з перших успішних прикладів монетизації відкритих даних у медицині. Також, крім реєстрів НСЗУ, використовуємо європейські інструменти для оцінки медико-санітарної грамотності, рекомендовані МОЗ та ВООЗ. Якими уже користуються в 35 країнах.

Завдяки співпраці з МІС, які інтегровані з eHealth, медбот Марта дозволяє знизити навантаження на лікаря. Через Бот можна записатися до лікаря, отримати повідомлення про запис на прийом, нагадування щодо планових щеплень, інформування про готовність лабораторних досліджень. В Марті окремо є функціонал для інформування пацієнтів про їхні права. Також є окремий розділ, присвячений профілактиці захворювань.

*- Як користуватися Ботом Марта?*

Сергій: Наразі аудиторія боту – 35 000 користувачів. Підключитись, до боту дуже просто – треба перейти за посиланням на сайт – <https://martabot.pro> та обрати зручний месенджер для комунікації. Реєструватись через сайт не потрібно – одразу вибираєте месенджер і далі сценарій, по якому буде надаватись інформація конкретно по вашому регіону.

Наразі доступна комунікація через Viber, Telegram, Facebook Messenger. Доступне безкоштовне використання по всій Україні.

*- Чи аналізували ви основну аудиторію користувачів? Якого віку люди найчастіше цікавляться Мартою?*

Сергій: Основна аудиторія 25-45 років. Коли розпочали інформаційну кампанію про коронавірус – дізналися, що підлітки також є окремою групою користувачів боту.

До прикладу, ми раніше не думали, що їх так цікавить медична сфера. А тепер вони за допомогою боту мають змогу більше дізнатись про вакцини, права пацієнта, як вибрати лікаря. Це пов'язано з форматом комунікації боту з користувачами: ми використовуємо доброзичливі звернення, смайли та гарне графічне оформлення. Це максимально наближено до живого спілкування, і таким чином користувачі охоче спілкуються з ботом. Ми так само аналізували аудиторію і шукали цей баланс спілкування навіть серед вибору емодзі.

*- Як саме Бот Марта інтегровано з медичними інформаційними системами?*

Сергій: В МедБот Марта є частина функціоналу, який зв'язаний з МІС (нагадування про прийом, результати аналізів, запис до лікаря тощо), але є й послуги, які надаються незалежно від МІС. А саме – оцінка медсервісу, опитування щодо рівня медико-санітарної грамотності, відповіді на часті запитання щодо медреформи, права пацієнтів, підписка на індивідуальну розсилку тощо. Функціонал медботу дозволяє моніторити та аналізувати

якість медичного сервісу, економить фінанси та надає керівникам медзакладів та муніципалітетам нові інструменти для розбудови медичної інфраструктури.

Дмитро: Значна частина функціоналу медботу дійсно доступна всім користувачам, незалежно від МІС, міста чи області України. Але є частина, яка доступна лише в містах, де він інтегрований з МІС. Тому в наших планах зробити всі функції бота доступними для всіх українців.

*- Як в умовах пандемії COVID-19 ви адаптували функціонал Марти?*

Вікторія: В кінці березня, коли була незрозуміла ситуація навколо нового вірусу, як і для жителів, так і для лікарів потрібно було розповісти про те, що таке коронавірус і як себе захистити.

Тоді ми розпочали інформувати ще й про коронавірус. Можна було перевірити статистику, як в світі, так і в Україні та певних містах. Проте, з аналізу розсилок ми зрозуміли, що таке інформування згодом стало неефективним, тому ми постійно адаптуємо зміни в функціоналі відповідно до запитів користувачів.

Комунікація в Марті проводиться на основі аналізу світового досвіду та рішень, які ми застосовуємо в нашому функціоналі. Регулярно проводимо опитування серед наших прихильників та втілюємо найцікавіші рішення, запропоновані користувачами. Таким чином, сервіс розбудовується відповідно до запитів самих користувачів, щоб нести для них максимальну цінність.

Марта дозволяє робити розсилку та опитування серед понад 30 000 осіб. Це в свою чергу дозволяє робити репрезентативну вибірку по регіонам/віку/статі бачити результати роботи медзакладів та ефективно оцінювати ключові тенденції.

*- Чи помітили ви позитивне ставлення в пацієнтів до медреформи після впровадження боту? Можливо, більша кількість населення почала укладати декларації?*

Дмитро: Подання інформації про медреформу в боті було цілком доступним та зрозумілим, тому прочитавши це, більшість користувачів підписали декларації. В умовах пандемії частина боту, де інформується про первинну ланку досі залишається актуальною. І про декларації, і про медичні послуги ми також досі інформуємо. Та наразі розширюємо функціонал стосовно переваг підключення вторинної ланки до реформи. Ми бачимо, що саме це інформування повертає довіру до лікарів і до медицини в цілому.

*- Розкажіть, будь ласка, про майбутні плани Мед боту Марта.*

Сергій: Більшість ідей нам підказали самі користувачі. Ми популяризуємо електронний кабінет пацієнта за рахунок сервісу «Медбот Марта». Щоб організація прийому була зручною та комфортною для всіх. Це допомагає контролювати скупчення людей і навантаження на лікарів та медзаклади.

Також плануємо розвивати сервіс на загальнонаціональному рівні. Активно ведемо розробку функціоналу спільно з медичними інформаційними системами.

Плануємо масштабувати використання сервісів НСЗУ, щоб інформувати пацієнтів про сімейних лікарів. Наприклад, якщо пацієнт бажає укласти (чи переукласти) декларацію – буде видно, які лікарі є доступними в його місті або найближчих медзакладах. Якщо знаєте ПІБ лікаря, зможете дізнатися, чи є в нього вільні місця для укладення декларацій та одразу отримуєте інформацію про пакет документів, необхідні контактні дані, які потрібні для укладання.

Якщо лікар звільниться чи переїде – пацієнтові прийде повідомлення про необхідність переобрати сімейного лікаря. Доступно та повністю безкоштовно в будь-якому регіоні України (*Як розвивається mHealth в Україні? // <https://ehealth.gov.ua/2020/11/06/yak-rozvyvayetsya-mhealth-v-ukrayini>. – 2020. – 06.11*).

### **Денис Башлык, директор по связям с госорганами Ассоциации УКАБ:**

**Почему и как нужно менять подходы к хранению важных государственных данных.**

Уявіть, що в країні зникли бази Державного земельного кадастру. За одну мить країна залишилася без усієї інформації про землю та її власників. Уявили? Катастрофа – не інакше. А головне, що причиною такого колапсу може стати зовсім не стрибок напруги в електромережі. Проблеми можуть настати через застарілу проводку у державній машині.

Мова йде про тендерне законодавство та застарілі підходи, які гальмують модернізацію критичної інфраструктури, частиною якої і є бази Держгеокадастру. Особливої важливості питання зберігання «земельних» баз набуває якраз зараз – перед імовірним відкриттям ринку землі.

Як склалася така ситуація, і наскільки, розтиражована в інтернеті інформація про загрозу для баз даних Держгеокадастру, правдива.

Отже все почалося у 2018 році. Саме тоді Державне підприємство Центр Державного земельного кадастру (Центр ДЗК), яке є адміністратором Державного земельного кадастру і відповідає за функціонування його баз даних, повідомило про необхідність придбання нового серверного обладнання.

**Причина більш, ніж вагома** – гарантія на старі сервери спливає. Після її закінчення обслуговування серверів виробником закінчиться. Окрім цього, майбутню закупку було погоджено з Державним агентством з питань електронного урядування. У результаті, у бюджеті на 2019 рік було передбачено 42,5 млн грн на придбання нового обладнання.

Спеціалісти Центру ДЗК підготували технічне завдання на придбання зазначеного обладнання. Здавалося, залишилося останнє – провести тендер. 23 серпня 2019 року, Центр ДЗК розпочав процедуру закупівлі. Після того

почались довгі процедури оскарження зазначеного технічного завдання в Антимонопольному комітеті України. З кожним рішенням АМКУ технічне завдання суттєво корегувалося.

28 листопада 2019 року, електронною системою закупівель переможцем тендеру було визначено підприємство Компанія КИТ. Вартість закупівлі склала 37,8 млн грн. Вже 18 грудня Центр ДЗК уклав договір на постачання обладнання. Привезти нові сервери постачальник мав до 20 грудня 2019 року.

### *Далі розпочинається найцікавіше.*

По-перше, Компанія КИТ із запізненням майже на тиждень (26 грудня) привозить обладнання, але, як виявилось, те зовсім не відповідає технічному завданню. Адміністратор Державного земельного кадастру звичайно відмовляється приймати зазначене обладнання. А, оскільки бюджетні кошти не були використані, то, відповідно до законодавства, їх було повернено до держбюджету.

Ось тут коло замкнулось. Адміністратор Державного земельного кадастру повідомив листом Держгеокадастр про цю ситуацію. Держгеокадастр, у свою чергу, звернувся до Мінекономіки, як до Головного розпорядника бюджетних коштів – обладнання необхідно обов'язково придбати.

У відповідь – тиша. Тож на виході ми маємо патову ситуацію. Потрібне обладнання відсутнє, а, головне – гроші було повернуто у держбюджет. Отже, якщо навіть обладнання привезуть просто завтра, то, щоб його оплатити, потрібно буде починати всю процедуру закупки спочатку – з ухвалення Мінекономіки. Хоча на останній запит вони так і не відповіли.

Ситуація патова, але точно не безнадійна. Навіть без нових серверів бази Державного земельного кадастру залишаються під захистом резервних серверів. Вони забезпечують дублювання та архівацію інформації. Крім того, це обладнання залишається на гарантії виробника. Це, у свою чергу, дає необхідний час для придбання нового обладнання.

### **Але ж все таки – у чому суть проблеми?**

Все прозаїчно – у недосконалості законодавства щодо закупівель обладнання для об'єктів критичної інфраструктури. Саме через це виникають ситуації, коли некваліфіковані компанії з відсутністю відповідного обладнання можуть фактично поставити під загрозу існування критичної державної інформації.

Проте вихід є. Він у реформі не тільки механізму закупівлі обладнання для критичної інфраструктури, але й у зміні самого принципу зберігання таких важливих державних даних.

Так – мова йде про хмарні технології. По-перше, це позбавить нас від необхідності кожні декілька років закупати нове «залізо». По-друге, унеможливить збої, які можуть пустити дані про землю «за вітром». Такі важливі державні дані мають безпечно зберігатися «у повітрі» (*Земля в*

*воздухе // <https://biz.liga.net/ekonomika/prodovolstvie/opinion/zemlya-v-vozduhe>. – 2020. – 05.11).*

## **Блоги та соціальні мережі**

### **Галина Верцімаха, керівник напрямку адвокатування комунікаційної платформи «Ліга антитрасту»:**

**Майно, яке не використовує держава або місцева громада, може стати в нагоді підприємцям, що і прибуток отримують, і оренду заплатять. Держава, в свою чергу, може і зекономити кошти на його утриманні, і отримати від оренди хороші гроші. Але за умови, якщо віддаватиме майно в користування на вигідних умовах.**

Раніше таке майно могли отримати далеко не всі. Як правило це був «закритий ринок для своїх» – «везунчиком» був наблизений до орендодавця бізнес. Саме від орендодавця залежало чи проведе він конкурс на право оренди, та хто стане переможцем. З переліком майна, яке можна було взяти у користування, також могли ознайомитись лише свої.

**В лютому 2020 року набрав чинності новий Закон «Про оренду державного та комунального майна», що має змінити ситуацію. Тепер державне та комунальне майно (окрім приміщень це транспортні засоби, обладнання та устаткування) можна орендувати на відкритих аукціонах в системі Прозорро.Продажі. Потенційні орендарі можуть ознайомлюватись з усім майном. Орендодавці ж зобов'язані розміщувати в електронній системі переліки такого майна.**

На виконання положень Закону Уряд затвердив Порядок, який детально визначає механізм передачі в оренду майна. Однією з новел є також можливість поскаржитись на процедуру організації аукціону, дії учасників, орендодавців та операторів майданчиків до спеціальної Комісії з розгляду скарг та підготовки пропозицій. За Законом це постійно діючий колегіальний орган, що розглядає скарги та пропозицій стосовно організації і проведення аукціонів, у тому числі електронних аукціонів.

За затвердженням Урядом в липні 2020 року «Порядком подання, розгляду скарг та пропозицій стосовно організації та проведення аукціонів щодо передачі в оренду державного та комунального майна» до складу Комісії входять представники Мінекономіки, Фонду державного майна та адміністратора електронної торгової системи.

У жовтні 2020 року наказом Мінекономіки затверджено склад Комісії з шести учасників, її очолює заступниця Міністра економіки.

Тобто тепер, на відміну від процедур попередніх років, учасник аукціону, користувач інтернету, який не зміг взяти участь в аукціоні, орендодавець та оператор електронного майданчика можуть звернутися до Комісії зі скаргою. При чому як у паперовій, так і в електронній формі.

Законодавство не визначає вичерпний перелік питань, які можна оскаржити. Але із затвердженої форми скарги випливає, що це і відсутність інформації про лот на сайті оператора електронного майданчика,

недостовірні інформація про нього, порушення оператором електронного майданчика або орендодавцем вимог до проведення аукціонів, недопуск оператором майданчика до участі в аукціоні, неможливість подачі цінової пропозиції, наявність дискримінаційних умов в оголошенні про проведення аукціону та інші.

Такі скарги можна подати на адресу Мінекономіки, а Комісія розгляне їх протягом 20 робочих днів з дати реєстрації та може продовжити строк ще на 10 днів.

За результатом розгляду скарг, що можуть проходити за участі скажників, члени Комісії простою більшістю можуть прийняти рішення про наявність чи відсутність порушення порядку організації, проведення аукціонів та вжиття заходів для усунення таких порушень. Таке рішення після затвердження протоколом Комісії надається відповідному орендодавцю, оператору електронного майданчика для розгляду та вжиття відповідних заходів. Витяг також оприлюднюється на офіційному веб-сайті Мінекономіки.

Окрім того, що рішення Комісії є обов'язковими до виконання, законодавство не визначає чітких строків його виконання.

Але цей механізм допоможе всім учасникам організації та проведення аукціонів з оренди державного та комунального майна захистити свої права.

Крім скарг, до Комісії також можна звертатись із пропозиціями, після розгляду яких Комісія рекомендуватиме удосконалити процес проведення аукціонів.

Поки що у відкритому доступі відсутня інформація про результати розгляду скарг на аукціони оренди державного майна. Вже з їх появою можна буде аналізувати які проблемні питання найчастіше виникають, як їх пропонують вирішувати та чи є ефективною робота Комісії (*Аукціони оренди майна на «Прозорро.Продажі» оскаржуються до Комісії Мінекономіки // <https://blog.liga.net/user/gvertsimakha/article/38477>. – 2020. – 23.11*).

### **Дмитрий Осыка, руководитель IT и программы цифровой трансформации MODUS, ДТЭК:**

**Технологии – лишь инструмент для цифровой трансформации, но успех преобразования зависит от трансформации культурной.**

Давайте представим себе ситуацию. У вас трое сотрудников и стоит задача, например, повесить картинку на бетонную стену. Для работы людям вы предоставили по одному инструменту – кому-то ручной молоток, кому-то дрель, а кому-то мощный перфоратор со всеми нужными насадками. Как думаете, кто справится быстрее и качественнее с заданием? У кого в распоряжении лучше инструмент? Возможно. Но важный момент – человек должен понимать и уметь им пользоваться, иначе речь идет не о пользе технологии в работе, а о бесполезности, или даже вреде.

От этого простого примера можно провести параллели и со значительно более сложным процессом цифровой трансформации. Цифровая



трансформація – это радикальное переосмысление того, как организация использует технологии, людей и процессы, чтобы коренным образом изменить эффективность своего бизнеса и удовлетворить потребность клиентов.

**Цифровая трансформация** – это не только технологии, а быть цифровой организацией означает не только использовать цифровые продукты, услуги и взаимодействие с клиентами. Технологии – инструмент, который позволяет сотрудникам в частности работать эффективнее и в лучших условиях, а бизнесу в целом усиливать основные операции. Но цифровая трансформация может закончиться так и не начавшись, если сотрудники компании не понимают зачем, как и что происходит. Поэтому, при трансформации компании в цифровую, требуются и большие изменения в действиях сотрудников, их собственном поведении и взаимодействии с другими людьми, внутри и вне организации. Иными словами, успешная цифровая трансформация начинается с культурной трансформации.

**Под цифровой культурой** в этом случае подразумевается некий набор принципов и ценностей в корпоративной культуре, характеризующих использование технологий для взаимодействия с обществом и решения задач в профессиональной деятельности. По сути, это установки или некий негласный кодекс того, как все происходит в компании, который дает сотрудникам свободу мнений и принятия ситуативных решений. Цифровая культура подразумевает повышение уровня цифровых навыков сотрудников, грамотности и умений пользоваться современными технологиями и программным обеспечением с учетом всех возможностей, которые дает информационный прогресс.

Универсальной формулы для формирования цифровой культуры нет. Имеют значение множество факторов – от размеров компании до отрасли или даже страны, в которой работает бизнеса. Но можно обратить внимание на **10 принципов для формирования цифровой культуры:**

1. Клиентоориентированность: в центре всех направлений деятельности – клиент или пользователь, сотрудники при разработке продуктов или услуг ставят себя на место клиента. Цифровая трансформация, где внедряются технологии ради них самих, обречена.

2. Ценностный подход: приоритезация при разработке продуктов и решений на основе ценности.

3. Работа на основе данных: в цифровой культуре обеспечено качество данных и информации, и решения принимаются на основе data.

4. Открытость к радикальным изменениям (disruption): работники открыты для решений, которые в корне меняют привычные бизнес-модели.

5. TL-подход (test and learn): поощряется смелость, а не осторожность. В цифровой культуре людям предлагается рисковать, анализировать неудачи, учиться на ошибках.

6. Динамика принятия решений: сотрудники действуют и реагируют быстро, акцент на действиях, а не на планировании. В быстро меняющемся

цифровом мире планирование и принятие решений должны переходить от долгосрочного к краткосрочному.



7. Для того, чтобы повысить динамику, нужно расширить права и возможности для сотрудников: работники должны получать автономию для принятия собственных решений.

8. Открытость: коммуникации между различными уровнями в иерархии – прямые и честные. Очень важный пункт – это трансформация «вертикальной» коммуникации ( по иерархии – сверху вниз) на «горизонтальную», контроля – на делегирование.

9. Коллаборация: работа в кросс-функциональных командах, сотрудничество ценится больше, чем индивидуальные усилия. Успех в цифровой культуре происходит благодаря коллективной работе и обмену информацией между департаментами, подразделениями и функциями.

10. Формирование экосистемы: компания развивается вместе с конкурентами, партнерами, внешним миром.

Все было бы намного проще, если бы культурная трансформация происходила быстро. Но формировать цифровую культуру нужно постепенно и важно быть готовым, что это длительный процесс. В ДТЭК, в рамках программы цифровой трансформации MODUS, мы пошли путем создания отдельной структуры – Экспертного центра цифровых технологий, далее были сформированы кросс-функциональные команды с экспертами центра и традиционных компетенций бизнеса. Постепенно мы все больше сближаем

цифровую и традиционную экспертизу. Начинали в 2019 году мы с проектов в пяти модулях (направлениях бизнеса), сейчас в работе уже девять, и еще два планируются к запуску в 2021 году. В сентябре в корпоративном институте Academy DTEK мы запустили пилот специальной образовательной программы Digital Transformation Program для сотрудников компании, которые вскоре будут вовлечены в проекты по цифровой трансформации.

*Масштабирование цифровой культуры* – это всегда челендж. Тем более, что мы говорим об трансформации традиционной культуры, основанной на четкой иерархии и инструкциях, на цифровую, где делегирование, коллаборация, открытость и скорость принятия решений играют важную роль.

Меняется нужно, в том числе и для того, чтобы оставаться актуальным. Например, согласно опубликованным данным IDC, несмотря на проблемы с бюджетом, вызванные вспышкой COVID-19, глобальные расходы на технологии и услуги цифровой трансформации в 2020 году все равно вырастут на 10,4 % до 1,3 триллиона долларов. Связано это с тем, что большинство реализуемых крупномасштабных проектов являются инструментами для более широкой бизнес-стратегии. Мы уже живем в цифровом мире, он будет развиваться и в будущем. Закладывая основы и развивая цифровую культуру сейчас, компании инвестируют в том числе и в свои конкурентные преимущества, долгосрочную и устойчивую работу (*Почему в вопросах цифровой трансформации нужно говорить о культуре?* // <https://blog.liga.net/user/dosyika/article/38451>. – 2020. – 19.11).

### **Владислав Криклій – міністр інфраструктури України:**

#### **Які новини у нас в цифровій інфраструктурі?**

Сьогодні ми працюємо паралельно над більш ніж 30 цифровими проектами, і наведу деякі приклади нашої роботи та які є новини.

#### ***Транспортний портал електронних послуг***

На сьогодні через транспортний портал електронних послуг <https://e-transport.gov.ua> видали вже більш ніж 530 000 дозволів на міжнародні вантажні перевезення. Ми постійно працюємо щодо отримання нових міжнародних дозволів, але, на жаль, часто кількість не залежить від МІУ.

#### ***Зважування у русі WIM***

Станом на зараз ми на завершальному етапі впровадження Weigh Control System, що забезпечуватиме автоматичний збір даних з WIM (Зважування у русі), портів та стаціонарних комплексів габаритно-вагового контролю, фотофіксацію відмови та розподіл надходжень від штрафів.

Вже сьогодні система об'єднує стаціонарні вагові комплекси міст, вагові комплекси філій АМПУ, Морського торговельного порту «Южний» та стивідорних компаній, а також пілотні комплекси WIM. Наразі триває під'єднання вагових комплексів Бердянського морського торговельного порту та стивідорної компанії «Ольвія». Вся інформація буде передаватись до центральної системи, де ми в реальному часі будемо бачити всю статистику

та можливі похибки, які потребують реагування. Це надасть нам можливість поступово відійти від людського впливу та бачити реальну ситуацію. Інформацію можна переглянути за посиланням: <https://bi.e-transport.gov.ua/dwc>.

Сподіваємося також на прийняття у другому читанні відповідного законопроекту, що надасть можливість почати вже і в автоматичному режимі зважувати у русі, а також при порушеннях штрафувати, що допоможе нам зберегти наші дороги.

#### *Учбовий центр i-Training ГЦЦК*

Відтепер i-Training

ДП «Галузевий центр цифровізації та кібербезпеки»

- перший та єдиний державний навчальний центр в Україні, який отримав статус Акредитованого навчального центру та академічного партнера компанії EC-COUNCIL, що надало можливість проводити навчання за всесвітньовідомими сертифікованими навчальними програмами в сфері кібербезпеки.

I-Training може проводити авторизоване навчання за напрямком Інформаційної безпеки та кібербезпеки за програмами міжнародних відомих вендорів: EC-COUNCIL, CompTIA, ISACA. Це дає можливість фахівцям МІУ отримувати нові навички для удосконалення свого досвіду та проводити навчання за міжнародними програмами також для інших державних органів, академічних закладів та приватного сектору.

Отримання сертифікації від EC-Council – це незаперечний доказ високої кваліфікації та глибоких технічних знань експертів-інструкторів, що працюють з i-Training та також допомагають в створенні електронних рішень МІУ

#### *SmartTicket*

На сьогодні SmartTicket працює у пілотному режимі на потягах далекого сполучення Укрзалізниці та у Київському міському транспорті. На цьому тижні розпочнемо також тестування взаємодії з системами SkyUp, а на наступному тижні будемо тестувати приєднання до системи приміської сполучення Укрзалізниці. Також розпочинається співпраця з Uklon, Bolt та Gansel.

Продовжуємо працювати над розвитком цифрових рішень, щоб поступово зменшувати вплив людського фактору на процеси та максимально спростити та автоматизувати отримання потрібних документів та дозволів (<https://www.facebook.com/vladkryklii>. – 2020. – 17.11).

#### **Артем Коханевич, CEO, GigaCloud:**

**Онлайн-образование в Украине оставляет желать лучшего. Нужен ли школе сервер и как обезопасить экзамены от списывания – могут подсказать облачные операторы.**

В современных реалиях рынок часто говорит о массовой миграции бизнеса в онлайн и повальной диджитализации процессов. Но мало кто

анализирует, как волны локдауна влияют на остальные сферы жизни. Уже сейчас стоит обратить внимание, например, на то, как будет меняться сфера образования, вынужденно подстраиваясь под новые реалии. И, возможно, помочь ей совершить качественный скачок, от которого в итоге выиграют все.

Отчет Всемирного экономического форума свидетельствует – за период пандемии количество работодателей, которые стали обучать персонал в режиме онлайн, увеличилось в пять раз. А число людей, ищущих возможности для обучения в Интернете по собственной инициативе, выросло в четыре раза.

Интересно, что несмотря на серьезный рост онлайн-обучения в бизнес-сегменте, государственные программы по онлайн-обучению выросли стремительнее рынка. Количество учащихся, получающих доступ к онлайн-обучению через государственные программы, за период пандемии выросло в девять раз и продолжает расти. И здесь госсектору удалось обогнать бизнес только по той причине, что большая часть образовательных инициатив в мире все еще лежит на плечах государственных институций.

Команда WEF также отмечает, что согласно изучаемым тенденциям, государства вскоре могут начать оплачивать прохождение онлайн-обучения, как одного из инструментов госполитики в сфере переподготовки и повышения квалификации кадров. И я считаю, что это будет очень хорошим решением, с учетом того, что в ближайшие годы нас ждет необходимость перепрофилирования большого количества кадров – из-за развития технологий, автоматизации и нового витка промышленной революции устареет множество профессий.

*Диджитализация образовательного процесса закономерно приводит учебные заведения к идее облачных технологий.* Ведь образование, перенесенное в облака – классический пример структуры с нагрузкой на вычислительные мощности 10 из 12 месяцев в году. Ее сложно прогнозировать и балансировать из-за различного ПО, используемого для курсов и лабораторных работ, а также разного количества студентов на разных курсах.

Круглогодично содержать ИТ-структуру, позволяющую спокойно работать на пике мультизадачности – финансово невыгодно. Ведь это не только оборудование (и затраты на электроэнергию), но и большое количество обучающих программ, не все из которых учебное оборудование позволяет устанавливать одновременно. А еще – существенное количество трудочасов преподавательского состава, вынужденного заниматься установкой и удалением программ. Ряд курсов до сих пор требует специальной подготовки рабочих мест студентов, из-за чего некоторые преподаватели тратят свои выходные на постоянную переустановку операционных систем и сопутствующего ПО.

Оценив объем затрат при физическом развертывании собственных ИТ-систем, почти 70 % высших учебных заведений Северной Америки уже перенесли или находятся в процессе перемещения своих систем в облако.

Модели услуг IaaS (инфраструктура как услуга) и SaaS (программное обеспечение как услуга), по сути, идеальны для решения проблем как высшего, так и школьного образования. Такие продукты обеспечивают образовательным заведениям работу на одном уровне с большими корпорациями, но без необходимости строить дорогую инфраструктуру.

При этом грамотный подход к масштабированию облачных ресурсов позволит образовательным заведениям одного типа дополнительно экономить на лицензиях, совместном использовании хранилища данных и т.п.

Мы как-то посчитали, что организация «школы в облаке» с надежным доступом учеников к онлайн-расписанию и базе учебных материалов, с возможностью проведения онлайн-уроков – обойдется администрации где-то в 12-15 тыс. грн в месяц из расчета на тысячу учеников. И эти деньги с лихвой компенсируются хотя бы сэкономленным временем персонала.

Для университетов требуется чуть более сложная инфраструктура и гораздо больше отдельных программных продуктов. Но и уровень финансирования высшего образования лучше, чем у школ. Дополнительный серьезный бонус использования облачных систем для организации, например, экзаменационного процесса – то, что «облака» намного лучше защищены от взлома и хакерских атак.

К сожалению, в Украине с онлайн-образованием все печально: согласно опросу, проведенному службой образовательного омбудсмена, учителя более чем половины украинских школ не имеют возможности дистанционно вести занятия из-за отсутствия необходимой техники у них дома. Почти половина учеников жалуется на низкую скорость интернета, а у 10 % из них дома до сих пор нет компьютеров. При этом, учителя жалуются на недостаточную мотивированность детей к учебе, а родители – на недостаточный контроль за состоянием усвоения знаний со стороны педсостава.

Также стоит отметить весьма низкое качество специализированного ПО для образовательного процесса. Далеко не все образовательные заведения смогли реализовать банальный контроль за переключением страниц при просмотре обучающего видео. Кроме того, в связи с противопандемическими карантинными мерами нагрузка на сайты школ и ВУЗов резко выросла, и ученики стали массово жаловаться на «подвисание», нередко приводящее к занижению оценок из-за невозможности вовремя завершить начатое тестирование.

Есть и обратные примеры. Один из наших клиентов – компания TATL Technology, реализующая проект «Единая Школа» – реализовала весь контроль за процессом обучения через электронную систему еще до начала карантина. Это позволило высвободить для учителей дополнительное время, которое они теперь могут потратить на повышение квалификации, а и

департаменту освіти – отримувати загальну картину освітнього процесу в режимі реального часу.

Система «Єдина школа» вже працює в столиці та в ряді областей України. Вона повністю відповідає законодавству та потребам шкіл, має рекомендацію Міністерства освіти та науки України та аттестат комплексної системи захисту інформації за рахунок розміщення в нашій хмарі. Цей проект, по суті, створює єдину інформаційну електронну середовище з участю учнів, їхніх батьків, педагогів та регіональних управлінь освіти.

На прикладі «Єдиної Школи» дуже добре видно, що може дати хмарний оператор освіті в Україні. Це можливість працювати добре та спокійно, забезпечувати вчителів та учнів усіма необхідними матеріалами саме тоді, коли це необхідно. Це спосіб підвищити якість освіти за рахунок покращення навчальних програм, доступності контенту та професійних систем моніторингу та контролю. І все це – в максимально гнучкому форматі, що дозволяє включати необхідні та відключати не потрібні модулі буквально в кілька кліків (*Діджиталізація онлайн-освіти – ще один хмарний тренд // <https://blog.liga.net/user/akohanevich/article/38410>. – 2020. – 13.11*).

**Александр Вернигора, директор компанії «Integracy Deals», глава підкомітету СУП по питаннях електронного документообігу та електронних довірливих послуг:**

**Закінчення терміну дії старих ЕЦП викликало невеликий переполох та багато питань. Коротко на них відповідаю.**

Нічого особливого або несподіваного не сталося. Ще два роки тому стало відомо, що після 7 листопада 2020 року старі ЕЦП втрачуть свою силу. Розмова йде про електронні підписи, отримані відповідно до Закону «Про електронний цифровий підпис». 7 листопада 2018 року йому на зміну прийшов Закон «Про електронні довірливі послуги» та термін дії ЕЦП, виданих до його набуття сили, був обмежений двома роками.

Що тепер буде з документами, підписаними старими ЕЦП? З ними все в порядку. Вони по-прежнему легітимні.

*Що змінилося для людей, які отримали свої підписи після листопада 2018?* Рівним чином нічого. Єдине, що слід зробити – перестати використовувати абревіатуру «ЕЦП». Так електронні підписи називалися до набуття сили Законом «Про електронні довірливі послуги». Відповідно до нового Закону правильно говорити «КЕП» – кваліфікована електронна підпись.

*Ще одне питання, яке турбує наших громадян: правда чи, що тепер КЕП можна зберігати тільки на захищених носіях?*

Відповідь: ні зовсім. В Законі чітко визначено коло осіб, які зобов'язані зберігати КЕП на апаратно-програмних пристроях, що забезпечують захист даних від несанкціонованого доступу. Це: «органи державної

влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, державні реєстратори, нотаріуси та інші суб'єкти, уповноважені державою на здійснення функцій державного реєстратора». Все остальное вправе сами решать, где хранить свои КЭП. Некоторые считают, что пользоваться защищенными носителями неудобно, и это – излишняя предосторожность. Возможно. Но это так же неудобно, как пользоваться замком на входной двери в квартиру. Лишняя мера предосторожности не мешает. Альтернативный вариант – Mobile ID. В этом случае КЭП хранится на защищенной SIM-карте вашего смартфона, и она всегда при вас.

*И последний вопрос:* когда закончится эксперимент с «усовершенствованной электронной подписью», которую можно хранить на любом носителе информации? В Постановлении Кабинета министров Украины №193 от 3 марта 2020 года определено, что тестовый период эксплуатации усовершенствованных подписей закончится до конца 2021 года: «Экспериментальный проект реализуется до дня набрания чинности змінами до Закону України „Про електронні довірчі послуги» щодо врегулювання використання удосконалених електронних підписів і печаток, які базуються на кваліфікованих сертифікатах відкритих ключів, але не пізніше ніж до 31 грудня 2021 року».

Следим за изменениями в законодательстве (*Электронная подпись старого образца больше не действительна. Что делать? // <https://blog.liga.net/user/avernyhora/article/38383>. – 2020. – 10.11*).

### **Иван Кучер, адвокат:**

**Нещодавнє рішення Конституційного Суду України продовжує перебувати «у топі» тем для правових і «не дуже» дискусій.**

У цей же час суб'єкти декларування намагаються зрозуміти, яким чином існувати в нових умовах та де та межа, за якою починається правопорушення.

Заходи фінансового контролю стосовно публічних службовців є «наріжним каменем» антикорупційної діяльності держави.

**Основним напрямом, звичайно, є так зване е-декларування та пов'язані із ним додаткові заходи, зокрема повідомлення про суттєві зміни в майновому стані.**

Відповідно до положень частини 2 статті 52 Закону України «Про запобігання корупції», у разі суттєвої зміни у майновому стані суб'єкта декларування, а саме отримання доходу, придбання майна або здійснення видатку на суму, яка перевищує 50 прожиткових мінімумів, встановлених для працевдатних осіб на 1 січня відповідного року, зазначений суб'єкт у десятиденний строк з моменту отримання доходу, придбання майна або здійснення видатку зобов'язаний повідомити про це НАЗК. Зазначена інформація вноситься до Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, та оприлюднюється на офіційному веб-сайті НАЗК.



З початку роботи системи е-декларування восени 2016 року і дотепер саме неповідомлення або несвоєчасне повідомлення про суттєві зміни в майновому стані є найрозповсюдженішим порушенням, яке допускають декларанти.

Про назване свідчить і судова практика у справах про адміністративні правопорушення, пов'язані з корупцією.

Однак, Рішенням Конституційного Суду України у справі за конституційним поданням 47 народних депутатів України щодо відповідності Конституції України (конституційності) окремих положень Закону України „Про запобігання корупції», Кримінального кодексу України № 13-р/2020 від 27.10.2020, визнано такою, що не відповідає Конституції України (є неконституційною), частину 2 статті 52 Закону України «Про запобігання корупції».

Зазначені положення Закону втрачають чинність з дня ухвалення Конституційним Судом України цього Рішення, тобто з 27.10.2020.

Тобто норма, за невиконання або неналежне виконання якої декларанти притягувались до відповідальності за частиною 2 статті 172-6 КУпАП, визнана такою, що не відповідає Конституції України та втратила чинність.

З огляду на те, що цитоване положення частини 2 статті 52 Закону №1700 безпосередньо застосовувалось судами під час розгляду справи вказаної категорії, оскільки саме за порушення положень цієї норми судом особи притягувались до відповідальності, визнання цієї норми неконституційною впливає на суть прийнятих рішень та може, на думку автора, слугувати підставою для перегляду таких судових рішень в якості виключної обставини.

#### ***Обґрунтування цієї позиції засноване на такому.***

Частина перша статті 55 Конституції України зобов'язує суди приймати заяви до розгляду навіть у випадку відсутності в законі спеціального положення про судовий захист.

Названа норма Конституції України відповідає зобов'язанням України, які виникли, зокрема, у зв'язку з ратифікацією Україною Міжнародного пакту про громадянські та політичні права, Конвенції про захист прав і основних свобод людини (Рим, 1950 рік), що згідно зі статтею 9 Конституції України є частиною національного законодавства України.

На це вказується також у Рішенні Конституційного Суду України від 25.12.1997 № 9-зп, згідно з яким відмова суду у прийнятті позовних та інших заяв, скарг, оформлених відповідно до чинного законодавства, є порушенням права на судовий захист, яке згідно зі статтею 64 Конституції України не може бути обмежене.

Відповідні рішення Конституційного Суду України констатують можливість перегляду та оскарження судових рішень у всіх випадках, крім тих, коли закон містить пряму і конкретну заборону на такий перегляд та оскарження.

Рішенням Європейського суду з прав людини від 1976 року у справі «Енгель та інші проти Нідерландів» суд закріпив висновки, що для цілей Конвенції про захист прав людини та основоположних свобод, поняття «кримінальне обвинувачення» має автономне значення, а не обмежується лише кваліфікацією «криміналу» згідно з національним законодавством, встановивши окремі критерії для визначення поняття «кримінальне обвинувачення» – *так звані «критерії Енгеля»*:

- критерій національного права, тобто, чи підпадає певне протиправне діяння під ознаки злочину згідно з національними нормами відповідної держави. Цей критерій є «не більше ніж відправною точкою», а отримані таким чином відомості мають лише формальну цінність;

- критерій кола адресатів, тобто якщо відповідальність поширюється на невизначене коло осіб, то правопорушення підлягає кваліфікації як кримінальне;

- критерій мети та тяжкості наслідків: разі, якщо у санкції наявний саме елемент покарання, а передбачені санкції є достатньо суворими, скоєне правопорушення розглядається за природою кримінального злочину.

Застосування згаданих критеріїв для оцінки кваліфікації порушення/обвинувачення як «кримінального» має на меті встановити наявність для особи додаткових гарантій, передбачених Конвенцією та задля невиконання яких (спрощення процедури до притягнення до відповідальності тощо) державою застосовано інший порядок, аніж встановлений кримінальним та кримінально-процесуальним законом.

Аналізуючи практику ЄСПЛ («Лутц проти Німеччини», «Карелін проти Російської Федерації», «Гурепка проти України», «Лучанінова проти України» та інші справи) у контексті застосування до проваджень у справах про адміністративні правопорушення «критеріїв Енгеля», зазначаємо, що значну роль у розширенні сфери застосування п. 2 ст. 6 Конвенції грає тлумачення двох ключових понять цієї статті – «кримінальне обвинувачення» і «суперечки про громадянські права». У справі «Кадубец проти Словаччини» представник держави-відповідача наполягав на тому, що в цій справі йдеться про адміністративний проступок, а не про кримінальне звинувачення, і, отже ст. 6 не може бути застосована. Однак Європейський суд з прав людини не погодився з аргументом відповідача, хоча і визнав, що внутрішнє право країни не вважає кримінальними діяння, за вчинення якого був покараний заявник. Проте ця обставина, на думку Суду, не має великого значення, так само як і те, який державний орган розглядав справу.

Аналізуючи крізь призму «критеріїв Енгеля» негативні наслідки у разі притягнення до відповідальності за вчинення правопорушень, пов'язаних з корупцією, передбачених частиною 2 статті 172-6 КУпАП, зауважую, що за наведеними критеріями мають застосовуватись правил та гарантії, визначені в якості обов'язкових до дотримання у провадженнях по кримінальним обвинуваченням.

Зокрема, аналіз диспозиції та санкції ч.2 ст. 172-6 КУпАП дає підстави стверджувати те, що це правопорушення відповідає критерію кола адресатів та критерію мети та тяжкості наслідків.

Такі висновки ґрунтуються на суворості стягнення/покарання за вчинення таких діянь, за змістом та розміром тотожні кримінальному покаранню у вигляді штрафу, а так само іншими негативними наслідками, передбаченими профільними законами «Про державну службу», «Про запобігання корупції», тощо (як приклад, заборона особі, яку притягнуто до відповідальності за правопорушення, пов'язані з корупцією, займати посади державної служби протягом трьох (!!!) років з дня притягнення до відповідальності), які за своїм змістом тотожні окремим кримінальним покаранням (позбавлення права обіймати певні посади або займатись певною діяльністю) та окремим кримінально-правовим наслідкам (судимість).

Наведене вказує на те, що при розгляді зазначеного вище правопорушення повинні застосовуватись принципи кримінального судочинства.

За таких обставин автор вважає, що провадження у справах про адміністративне правопорушення, передбачене частиною 2 статті 172-6 КУпАП, вважається кримінальним у розумінні Конвенції про захист прав людини і основоположних свобод, до нього мають застосовуватись норми кримінального процесуального законодавства, які передбачають перегляд рішення за нововиявленими обставинами та містять перелік даних обставин.

Відповідно до положень статей 459 та 460 КПК України судові рішення, що набрали законної сили, можуть бути переглянуті за виключними обставинами за відповідною заявою учасників судового провадження.

Відповідно до пункту 1 частини 5 статті 461 КПК України, заяву про перегляд судового рішення за виключними обставинами може бути подано протягом тридцяти днів із дня офіційного оприлюднення рішення Конституційного Суду України, яким встановлено неконституційність закону, іншого правового акта чи їх окремого положення, застосованого судом при вирішенні справи.

Очевидно, що визнання неконституційною норми, за порушення якої особи притягувались до відповідальності, є виключною обставиною, а з урахуванням «кримінальної» суті названого правопорушення, заяви про перегляд судових рішень у таких справах мають розглядатись судами із застосуванням положень кримінального процесуального законодавства.

Наразі Єдиний державний реєстр судових рішень не містить рішень у такій категорії справ, на підставі яких судову практику можна було б проаналізувати.

Однак зважаючи на «активність» правоохоронців у попередніх роках, очікується значна кількість заяв про перегляд постанов за частиною 2 статті 172-6 КУпАП на підставі рішення Конституційного Суду України № 13-р/2020 від 27.10.2020 (*Цікаві наслідки рішення КСУ від 27.10.2020 (щодо е-*

*декларування) // <https://blog.liga.net/user/ikucher/article/38375>. – 2020. – 09.11).*

**Надія Баловсяк, медіаексперт, журналіст:**

**На початку пандемії COVID-19 на додатки для відстеження контактів покладалась великі надії. Проте всі сподівання виявились марними.**

На початку пандемії COVID-19 багато експертів та уряди декількох країн були впевнені, що мобільні додатки для відстеження контактів допоможуть у боротьбі з пандемією. Після першої хвилі обурень з приводу того, що ці додатки можуть порушувати приватність користувачів, компанії Google та Apple розробили власні технології, які, з одного боку, гарантували приватність та захист користувацьких даних, а з іншого – дозволяли фіксувати контакти людей, і у випадку, якщо в одного з них виявиться COVID-19, то повідомляли б інших про необхідність самоізоляції. Більше того, обидві компанії дозволяли у своїх мобільних магазинах додатків лише ті, які використовували саме ці створені ними технології.

*Проте, ось друга хвиля захворюваності вражає все більше країн світу, ми жахаємося від статистики, а про мобільні додатки для відстеження контактів уже ніхто й не згадує.* Іншими словами, ця ідея повністю провалилась. Хоча вона й виглядала багатообіцяючою, в цій пандемії мобільні технології не лише не стали інструментом для її обмеження, вони практично ніяк не були використані в тому, щоб стримати COVID-19.

В деяких країнах світу офіційні додатки для відстеження контактів з'явилися лише ближче осені (як у Великобританії), то ж говорити про їх ефективність чи неефективність рано. Але в інших країнах, де додатки були випущені набагато раніше, практично немає інформації про те, що ці додатки стали якимось помітним чинником в боротьбі з COVID-19.

**Мій смартфон – мої додатки**

На початках прогнозувалось, що навряд чи багато користувачів будуть встановлювати ці додатки на свої гаджети. Проте в оптимістичних прогнозах фігурували дані в 65 %-85 % користувачів. Насправді ситуація виявилась набагато гірша. У Німеччині додатки встановили біля 21 % користувачів, в Італії 14 %, у Франції лише 3 %, – повідомляє видання The Next Web. Першими такі додатки запустили Ісландія та Сінгапур, та й там доля користувачів, які встановили собі ці додатки, склала 40 %.

Активність використання таких додатків насправді напряму пов'язана з їх ефективністю. Чим більше людей користуються такими додатками, тим вони ефективніші, тобто тим більше взаємодій з носіями вірусу можуть зафіксувати. користуються 20 % користувачів, то у них є 4 %-й шанс контактувати з іншим користувачем програми. Хоча навіть проникнення у 40 % в Сінгапурі дозволило Міністерству охорони здоров'я Сінгапуру протягом двох днів замість чотирьох (до запуску додатків) виявляти коло контактів у людини, яка захворіла.

## Відсутність довіри?

Однієї з причин такого розвитку ситуації з додатками для відстеження контактів може бути відсутність довіри до самої технології та її використання персональних даних.

І, не дивлячись на те, що Google та Apple запропонували свої рішення, в деяких країнах скористались власними розробками. До прикладу, у Франції довго роздумували, чи повинна програма завантажувати дані в центральну базу даних чи зберігати їх на телефонах користувачів, вибрала першу систему і зіткнулась з тим, що додаток для відстеження контактів встановили лише 4 % користувачів.

Великобританія також спочатку експериментувала з централізованою моделлю, але після великої критики та повідомлень про труднощі перейшла на децентралізовану. Однак таке активне обговорення теж могло негативно вплинути на популярність додатків.

Справді, є вагомі причини скептично ставитись до ефективності цих додатків. Більшість країн (за винятком Ісландії) вирішили використовувати Bluetooth для того, щоб фіксувати взаємодію між користувачами, замість GPS для відстеження конкретного місцезнаходження. Цей вибір було зроблено з метою захисту конфіденційності. Але Bluetooth часом працює з похибками, може реєструвати контакти, яких ніколи не було, і пропускати реальні взаємодії.

Деякі дослідження порівняння ефективності цих додатків дійшло висновку, що вони часто працюють з великими похибками, і загалом їх принцип був дуже неточним, не кращим, ніж «випадкова вибірка» людей. Відповідно, помилкові сповіщення також не сприяли довірі до програм відстеження.

## Проблема технології

Окремою проблемою стало те, що цими програмами можуть користуватися лише власники смартфонів. І якраз основна група ризику – люди, старші 65 років, не зможуть скористатися програмами для відстеження контактів.

І це питання можна вирішити, наприклад, у Сінгапурі запропонували використовувати спеціальні мітки, які можна носити на ремінці або в кишені чи сумці, і яка дозволяє відстежувати контакти. У Новій Зеландії спробували використовувати з такою ж метою «картку covid».

Проте питання в тому – чи вибрати смартфон з додатком, чи вибрали брелок чи щось інше – якщо ця технологія існує окремо від загальної системи тестування та відстеження, то вона не буде працювати.

Українська «Дія вдома» так само не стала інструментом боротьби з пандемією – окрім примусового встановлення додатку для тих, хто повертається із закордону. Хоча цей додаток – це окрема історія (**Чому провалилась ідея боротьби з COVID-19 з використанням мобільних додатків // <https://blog.liga.net/user/nbalovsiak/article/38359>. – 2020. – 06.11).**

**Александр Вернигора, директор компании «Integracy Deals», глава подкомитета СУП по вопросам электронного документооборота и электронных доверительных услуг:**

**Внедрение новых технологий влечет за собой появление разных технических и юридических вопросов. Электронный документооборот – не исключение. Один из них – что считать «датой создания документа?»**

В Украине еще в 2003 году появилась возможность подписывать документы в электронном виде. Тогда был принят закон об электронной цифровой подписи. Позже, на смену ему пришел «Закон об электронных доверительных услугах». Но в законодательной базе Украины еще остаются моменты, которые требуют уточнения. Один из них – вопрос даты составления первичных электронных документов, в которых фиксируется как дата создания, так и метки времени наложения электронных подписей.

Наложение электронной подписи регламентируется «Законом об электронных доверительных услугах». При ее нанесении, формируется метка времени, которая фиксирует момент подписания. Очевидно, что метка времени и дата создания документа – разные понятия. В «Законе о бухгалтерском учете» есть определения даты и подписи, которые являются обязательными реквизитами, но о метках времени там ничего не сказано.

На бумажном документе отображается только дата его создания. Время подписания значения не имеет. В случае с электронными документами, кроме даты создания, фиксируется также метки времени: когда именно документ был подписан, как с одной, так и с другой стороны. Получается, что в электронном документе содержатся данные и о времени создания документа, и времени наложения электронных подписей. Они могут существенно отличаться. У многих представителей бизнеса возникает вполне резонный вопрос: если дата создания документа и дата подписи не совпадают, какое время контролирующие органы будут считать моментом возникновения налоговых обязательств по НДС?

Учитывая настороженное отношение к ЭДО со стороны финансовых отделов некоторых представителей бизнеса, необходимо прояснить этот вопрос раз и навсегда. Многие опасаются, что налоговые органы сочтут документ недействительным, если даты создания и подписи будут отличаться. Пока таких прецедентов нет, тем не менее, необходимо исключить вероятность того, что налоговая интерпретирует разницу в датах таким образом, что придется платить штраф.

Когда нет определенности, появляются неуверенность и страх. Как результат, финансовые отделы компаний начинают сопротивляться внедрению электронного документооборота. Если дата создания документа будет признана датой предоставления услуг, компании смогут спокойно переводить все свои документы в электронный формат. Этот вопрос необходимо решить, так как ни в налоговом кодексе, ни в разъяснительных документах Министерства финансов ответа на него нет.

Подкомитет по вопросам электронного документооборота и электронным доверительным услугам ИТК комитета «Союза украинских предпринимателей» решил взять инициативу в свои руки. Его участники предложили внести изменения в статью 187 Налогового кодекса Украины: «Для документов, составленных в электронной форме в соответствии с требованиями Закона Украины «О бухгалтерском учете и финансовой отчетности в Украине», датой оформления электронного документа, удостоверяющего факт поставки услуг плательщиком налога, считается дата составления такого электронного документа».

При осуществлении налогоплательщиком (поставщиком) операции по поставке услуг, которые оформлялись первичным документом составленным в электронной форме, датой возникновения налоговых обязательств по НДС по такой операции считается дата составления первичного документа, который содержит сведения о хозяйственной операции, независимо от дат наложения электронных подписей.

Сейчас вариант изменений предлагается в законопроекте № 4101 от 15 сентября 2020 года, который предусматривает внесение изменений в подпункт б) пункта 187.1 статьи 187 НКУ: «Для документов, составленных в электронной форме в соответствии с требованиями Закона Украины «О бухгалтерском учете и финансовой отчетности в Украине», датой оформления электронного документа, удостоверяющего факт поставки услуг плательщиком налога, считается дата составления такого электронного документа».

То, что законопроект № 4101 уже попал в Раду – безусловно, шаг вперед, но в нем также содержится много других, спорных поправок к законам. Остается надеяться, что парламентарии быстро разберутся со всеми поправками и до конца этого года вопрос с датой создания электронного документа будет решен (*Один акт – три даты. Что считать датой создания электронного документа* // <https://blog.liga.net/user/avernyhora/article/38306>. – 2020. – 02.11).

### **Надія Баловсяк, медіаексперт, журналіст:**

**Технологія розпізнавання відноситься до однієї з найбільш контрверсійних. З одного боку, вона дозволяє ідентифікувати людину, що спрощує пошук злочинців, з іншого – порушує право людини на приватність.**

Окрім того, це технологія, відмовитись від якої нам практично неможливо – про це пише авторка книжки «Капіталізм спостережень» Шошанна Зубофф. Ви можете, звісно, виходити з дому, повністю закривши обличчя, приховавши його масками, темними окулярами, шапками чи кепками. Але весь час так ходити ви не будете, окрім того, масове носіння масок (перепрошую за цю навмисну тавтологію) покращило роботу технологій розпізнавання – вони прекрасно впізнають людину навіть тоді, коли вона носить маску.

*Саме тому технології розпізнавання зіткнулись з технологічною стриманістю – ситуацією, коли регулятори та суспільство вимагають призупинити їх використання до того, як будуть зважені всі «за» та «проти», а ще – доки ці технології не будуть відрегульовані.*

У США, країні, яка значно поступається Європі повагою до приватного життя особистості, уже декілька міст заборонили використання технології розпізнавання – у вересні така заборона запрацювала у Портленді. Цього тижня така заборона почала діяти в Лос-Анжелесі. Влітку цього року декілька великих технологічних компаній (Amazon, IBM та Microsoft) запровадили мораторій та використання цих технологій. Правда, BigTech розуміють, що вони не можуть відмовитись від цих розробок, бо на цей дуже перспективний ринок прийдуть інші, то ж Amazon і Microsoft найняли лобістів після прийняття місцевих законів щодо заборони розпізнавання. Наразі не можна сказати достеменно, як ця технологія регулюватиметься у США, принаймні, на федеральному рівні, проте очевидно, що цей розвиток враховуватиме поради фахівців з безпеки та правозахисників.

Протилежний шлях застосування технологій розпізнавання обрали у Москві. Минулого тижня стало відомо, що страхові компанії ведуть перемовини з владою про прямий доступ до камер відеоспостереження – звісно ж, з благородною метою виявлення випадків шахрайства та вирішення спірних страхових випадків. До цієї новини варто додати ще одну – мерія Москви, яка давно використовує технології розпізнавання, в тому числі й для того, щоб моніторити хворих на Covid, замовила неперервний моніторинг активності жителів міста. Влада планує спостерігати за штрафами, боргами та «медичними обмеженнями». Для цього будуть створені профілі громадян, які міститимуть агреговану інформацію, ймовірно, теж отриману з розгалуженої мережі камер із розпізнаванням облич. Іншими словами, китайський соціальний рейтинг, про який роки два тому не написав лише лінивий, сподобався нашому північному сусідові.

Таким чином, ***ми можемо виділити два підходи до технологій розпізнавання*** – умовно-західно-американський, зі спробами зважати на базові права людини та намаганням розуміти ризики масового застосування такої технології, та умовно східний, реалізований в Китаї та такий, що має бути реалізований в Москві.

Питання в тому, який шлях для себе обере Україна, наразі відкритий і не можна виключати ймовірність того, що ми підемо китайсько-російським шляхом. Спостерігаючи, як працюють наші правоохоронці, в тому числі в справі по убивстві Павла Шеремети, щодо якої лише лінивий не прочитав вільне трактування правоохоронцями зображень із камер спостереження, можна припустити, в що може перетворитись спроба спостерігати та впізнавати всіх в Україні.

Часом звучать думки про те, що задля великих суспільних ідей (наприклад, для боротьби з пандемією) варто відмовитись або обмежити громадянські права. Ці твердження мають право на існування, проте не варто



забувати, що пандемії мають властивість завершуватися, але правоохоронці не мають звички відмовлятися від технологій спостереження за громадянами. Тому потрібно розуміти всі ризики технологій розпізнавання, особливо в умовах нашої країни *(Два підходи до використання технологій розпізнавання облич: який вибере Україна? // <https://blog.liga.net/user/nbalovsiak/article/38542>. – 2020. – 02.11)*.

## **Зарубіжний досвід**

Специальное подразделение цифровых рынков (Digital Markets Unit) будет создано в Великобритании в апреле 2021 года в Управлении по конкуренции и рынкам (Competition and Markets Authority), оно будет тесно сотрудничать с регулируемыми органами, чтобы запустить и обеспечить соблюдение нового кодекса для управления работой в стране доминирующих цифровых платформ, таких как Google и Facebook, сообщило министерство цифровых технологий, культуры, средств массовой информации и спорта Соединенного Королевства.

«Новый нормативный кодекс поведения будет означать, что потребителям будет предоставлен больший выбор и контроль над тем, как используются их данные, малые предприятия смогут лучше продвигать свои продукты в Интернете, а новостные агентства не будут вытеснены их более крупными конкурентами», – сказано в сообщении.

Как отмечает ведомство, онлайн-платформы приносят огромную пользу бизнесу и обществу, их услуги облегчают и ускоряют работу и помогают людям оставаться на связи друг с другом, миллионы людей делятся творческим контентом или рекламируют товары в Интернете. «Но в Великобритании и за рубежом растет консенсус в отношении того, что концентрация власти у небольшого числа технологических компаний сдерживает рост технологического сектора, сокращает количество инноваций и потенциально оказывает негативное влияние на людей и предприятия, которые полагаются на них», – сообщается в релизе.

Новое подразделение может быть наделено полномочиями приостанавливать, блокировать и отменять решения технологических гигантов, приказывать им предпринимать определенные действия для достижения соответствия кодексу и налагать финансовые санкции за несоблюдение (*Татьяна Костылева Власти Британии решили создать новую структуру по надзору за американскими цифровыми компаниями // <https://d-russia.ru/vlasti-britanii-reshili-sozdat-novuju-strukturu-po-nadzoru-za-amerikanskimi-cifrovymi-kompanijami.html>. – 2020. – 27.11).*

**В программу ускоренной блокировки доменов в Великобритании включено британское управление по контролю лекарственных средств и медицинских изделий (Medicines and Healthcare products Regulatory Agency – MHRA).**

Согласно этой программе регистратура Nominet, управляющая национальным доменом Великобритании, имеет право оперативно блокировать доменные имена, подозреваемые в причастности к противоправным действиям.

MHRA стало вторым британским государственным учреждением, включённым в программу ускоренной блокировки. Ранее программа распространялась только на отдел по борьбе с преступлениями в сфере интеллектуальной собственности полицейского управления Лондона.

MHRA является инстанцией, одобряющей использование в Великобритании лекарственных препаратов и изделий медицинского назначения (*Британское управление по контролю за оборотом лекарств получило право быстрой блокировки доменов // <https://d-russia.ru/britanskoe-upravlenie-po-kontrolju-za-oborotom-lekarstv-poluchilo-pravo-bystroj-blokirovki-domenov.html>. – 2020. – 26.11).*

Использование ещё 43 китайских приложений, включая сервисы для покупок от Alibaba Group, запрещено в Индии со вторника – «чёрный список» заблокированных китайских приложений превысил 200.

Вместе с AliExpress во вторник были заблокированы видеосервис Taobao Live, более десятка платформ для знакомств и игр. Ранее в Индии уже были заблокированы мессенджер WeChat от Tencent Holdings Ltd. и сервис обмена видео TikTok от ByteDance Ltd.

Индийское правительство заявило, что запреты обусловлены интересами национальной безопасности.

Ранее министерство электроники и информационных технологий Индии заявляло, что заблокированные приложения «крадут и тайно передают» данные пользователей на серверы за пределами Индии (*Индия заблокировала уже 200+ китайских приложений // <https://d-russia.ru/indija-blokirovala-uzhe-200-kitajskih-prilozhenij.html>. – 2020. – 25.11).*

Правительство Великобритании раскрыло подробности о своём новом киберподразделении – National Cyber Force, NCF, состоящем из «боевых хакеров», чьими мишенями станут «вражеские государства», прежде всего Китай и Россия, террористические группировки и «даже педофилы»; задачей NCF будет «нарушение онлайн-коммуникаций» указанных целей.

NCF, контролируемое Центром правительственной связи (Government Communications Headquarter, GCHQ) и Минобороны Великобритании, было сформировано и тайно приступило к операциям в апреле. В штате «несколько сотен» хакеров, работающих на нескольких военных базах по всей стране. За 10 лет численность «боевых хакеров» планируется довести до трёх тысяч.

На прошлой неделе премьер Борис Джонсон сообщил о 10-процентном увеличении финансирования военных расходов, отметив, что эти деньги выделяются на космические и кибероборонные проекты, в том числе на формирование национальных кибервойск для защиты населения от онлайн-угроз. Говоря об NCF, он заявил, что киберподразделение объединяет «наши

спецслужбы и военнослужащих» и уже проводит операции в киберпространстве против террористов, организованной преступности и деятельности вражеских государств.

Угрозу Великобритании в киберпространстве представляют около 60 стран, включая Иран, Северную Корею и, конечно же, Россию и Китай. О намерении GCHQ стать «киберорганизацией» и поставить защиту «цифрового отечества» во главу угла своей работы Центр сообщил еще три года назад.

Декларируется, что операции NCF должны получать одобрение министра иностранных дел или министра обороны, в зависимости от объекта нападения и требуемых ресурсов. Инсайдеры говорят, что в действительности NCF будет работать вне пределов существующего регулирования под контролем парламентского комитета по разведке и безопасности. Все операции NCF засекречиваются. Имя действующего руководителя NCF не называется, однако известно, что это сотрудник GCHQ, проработавший там более 20 лет (*Вика Рябова Великобритания раскрыла данные о киберподразделении «боевых хакеров» // <https://d-russia.ru/velikobritaniya-raskryla-dannye-o-kiberpodrazdelenii-boevyh-hakerov.html>. – 2020. – 23.11).*

**В совместном заявлении министров внутренних дел государств – членов Европейского союза, составленном по итогам внеплановой видеоконференции по борьбе с терроризмом в пятницу, 13 ноября 2020 года, поставлен вопрос о создании в Европейском союзе системы блокировки в Интернете информации, содержащей пропаганду терроризма, в течение часа с момента её обнаружения.**

Завершение переговоров о создании системы блокировки антитеррористического контента ожидается до конца 2020 года.

Министры внутренних дел выступили в поддержку разработки нового закона Европейского союза о цифровых услугах (Digital Services Act), направленного на усиление ответственности интернет-компаний за распространение противоправного контента в Интернете, а также запрещающего крупнейшим технологическим компаниям (Facebook, Google, Amazon, Apple и др.) создавать преференции для аффилированных с ними сервисов. В настоящий момент проект закона о цифровых услугах дорабатывается Европейской комиссией.

В совместном заявлении министров иностранных дел отмечено, что компании – операторы социальных сетей и мессенджеров должны собственными силами проводить более тщательный мониторинг контента и удалять «сообщения террористического и другого радикального характера» сразу после их обнаружения, не дожидаясь судебного решения. Также в совместном заявлении подчеркнута необходимость криминализовать в Европейском союзе пропаганду ненависти в Интернете.

Міністри пропонують розглянути питання доступу правоохоронних органів до зашифрованих даних користувачів, зокрема, до переписки. Мета – боротьба з тероризмом, забезпечення юридичної значимості отриманих даних та можливість їх представлення в судах як доказів.

*Згідно спільного заявлення* дані про осіб, які представляють терористичну загрозу, повинні бути внесені в єдину інформаційну систему, до якої матимуть доступ органи всіх держав – членів Європейського союзу. Крім цього пропонується розглянути питання розширення можливостей Шенгенської інформаційної системи (Schengen Information System, SIS) для обробки біометричних персональних даних осіб, які прибувають на територію Європейського союзу.

Відзначено, що для реалізації вищевказаних заходів в першу чергу необхідна організаційно-правова основа, зокрема, достатній обсяг фінансових та людських ресурсів. Міністри внутрішніх справ закликали держави – члени Європейського союзу сприяти взаємному міждержавному співробітництву як між собою, так і з державами, які не входять до складу Європейського союзу (*Александр Федотов ЕС может создать систему блокировки террористического онлайн-контента – итоги совещания глав МВД // <https://d-russia.ru/es-mozhet-sozdat-sistemu-blokirovki-terroristicheskogo-onlajn-kontenta-itogi-soveshanija-glav-mvd.html>. – 2020. – 20.11*).

Республіка Казахстан, як і Україна, успадкувала від радянського періоду систему охорони здоров'я, побудовану за моделлю Семашко, тобто охорона здоров'я перебувала у власності держави, функціонувала на основі централізованого планування, і одним з її ключових принципів був загальний і безкоштовний доступ населення до медичної допомоги.

Після здобуття у 1991 році незалежності Казахстану довелося розробляти власну політику і систему планування в галузі охорони здоров'я. Багато функцій Міністерства охорони здоров'я були децентралізовані і передані регіонам, обласні департаменти охорони здоров'я володіли значним ступенем самостійності.

На сьогодні медична система Казахстану адаптована до міжнародних стандартів, відповідно до базового набору стандартів та короткострокового плану стандартизації електронної охорони здоров'я.

Національна стандартизація в галузі електронного здоров'я регулюється технічним комітетом з стандартизації та комітетом з технічного регулювання та метрології Міністерства інвестицій та розвитку Республіки Казахстан.

**Стандартизація відбувалась у декілька етапів:**

- 2013-2014 роки – Створення електронної моделі медичної картки, яка включала перший базовий набір стандартів також визначили перші класифікатори в електронній системі охорони здоров'я.

Оскільки не було компетенції розробляти стандарти у галузі електронного охорони здоров'я, стандарти були прийняті у формі стандартних вимог та норм.

- 2015-2016 рр. – ідентифікація функціоналу електронної медичної картки, що включає процеси медичного обслуговування та визначення додаткових класифікаторів для їх підтримки. У 2015 році було розроблено та затверджено 4 стандарти та розпочався процес адаптації класифікаторів.

- Далі з 2017го по 2020 рік затвердили урядом стратегію розвитку електронної системи охорони здоров'я казахстану.

На сьогодні Урядом Республіки Казахстан ефективно здійснюється політика щодо розвитку і модернізації національної системи охорони здоров'я.

За роки реформ в сфері охорони здоров'я країни відбулися кардинальні зміни: удосконалили законодавство, прийняли нові державні та галузеві програми з питань розвитку національної системи охорони здоров'я (*eHealth в світі. Kazakhstan // <https://ehealth.gov.ua/2020/11/20/ehealth-v-sviti-kazakhstan>. – 2020. – 20.11*).

**Американские законодатели представили в среду законопроект, ужесточающий правила кибербезопасности для федеральных гражданских ведомств.**

Предложено внести поправки в закон 2015 года, уже предусматривающий такие меры киберзащиты госведомств, как шифрование данных и двухфакторная аутентификация пользователей информационных систем, и назвать новый документ «законом о надзоре за кибербезопасностью 2020 года».

Законопроект переходит от бессрочных отказов ведомств («отсрочек») от внедрения тех или иных мер кибербезопасности к отказам, действующим только один год, и упрощает надзор за соблюдением установленных правил информационной безопасности со стороны Конгресса для защиты федеральных сайтов, конфиденциальных данных и других важных систем от атак. Действующий же закон, по словам авторов нового законопроекта, позволяет агентствам бессрочно переносить внедрение технологий кибербезопасности.

Теперь, чтобы получить отсрочку, руководитель агентства должен подтвердить, что требование является «чрезмерно обременительным» для выполнения, или что нет необходимости обеспечивать безопасность системы и данных ведомства, и что агентство «предприняло все необходимые шаги» для обеспечения своей безопасности.

Документ также требует предоставления ежегодных отчетов госведомств в Конгресс, включая список конкретных отказов от внедрения технологий кибербезопасности, вместе с оценкой того, когда ведомство сможет выполнить требования кибербезопасности (*Татьяна Костылева В США ужесточают правила кибербезопасности для государственных*

*ведомств – законопроект // <https://d-russia.ru/v-ssha-uzhestochajut-pravila-kiberbezopasnosti-dlja-gosudarstvennyh-vedomstv-zakonoproekt.html>. – 2020. – 19.11).*

Странам Євросоюзу следует добиваться принятия нормы, согласно которой провайдеры будут обязаны в течение часа изымать радикальный контент, представляющий опасность для общества, заявил президент Франции Эмманюэль Макрон во вторник, выступая по итогам саммита ЕС, прошедшего в формате видеоконференции и посвящённой борьбе с терроризмом.

«В ходе саммита мы рассмотрели, в частности, необходимость вести решительную борьбу против пропаганды терроризма и порождающих ненависть высказываний в Интернете. Интернет и социальные сети – пространство свободы, однако эта свобода может существовать только с учётом фактора безопасности. Интернет не может становиться пристанищем для тех, кто попирает наши ценности и стремится обработать людей с помощью смертоносной пропаганды».

«Именно поэтому совершенно необходимо, чтобы уже в ближайшие недели был одобрен регламент изъятия в течение одного часа контента террористической направленности, – подчеркнул Макрон. – Это очень важно, и такая договоренность станет результатом той работы, которую мы в свое время начали летом 2017 года совместно с [бывшей в то время британским премьером] Терезой Мэй. Эта работа должна в ближайшие недели привести именно к указанным нами выше целям».

Он сообщил, что Франция поддерживает «намерение Европейской комиссии предложить в начале декабря новое законодательство, направленное на борьбу против контента, провоцирующего ненависть». Речь идет о так называемом законопроекте о цифровых услугах (*Digital Services Act, DSA*) (*Опасный интернет-контент следует изымать в течение часа – Эмманюэль Макрон // <https://d-russia.ru/opasnyj-internet-kontent-sleduet-izumat-v-techenie-chasa-jemmanjujel-makron.html>. – 2020. – 11.11).*

Совет Европейского Союза разослал на согласование представителям стран-участниц проект резолюции (*Draft Council Resolution on Encryption*), обязывающей операторов мессенджеров создавать и сообщать правоохранителям мастер-ключи для мониторинга чатов и сообщений, защищённых сквозным шифрованием.

Документ получен и опубликован, в частности, австрийской телерадиовещательной корпорацией ORF. Проект резолюции датирован 6 ноября, документ находится на согласовании и может быть принят на видеоконференции министров внутренних дел и юстиции стран ЕС в начале декабря без дальнейшего обсуждения.

Поводом для ускоренной разработки и принятия резолюции послужил теракт в Вене.

Как говорится в проекте резолюции, Евросоюз «полностью поддерживает разработку, внедрение и использование устойчивого шифрования», но в то же время требует, чтобы криптография не мешала компетентным органам исполнять свою работу офлайн или онлайн. В документе описаны опасности неконтролируемой криптозащиты каналов связи, которые преступники используют для общения.

«Компетентные органы должны иметь законный и адресный доступ к данным, не нарушающий фундаментальные права человека и политику защиты данных, а также принципы кибербезопасности. Технические решения для получения доступа к зашифрованным данным должны соответствовать принципам легальности, прозрачности, необходимости и пропорциональности. ...Согласно решению Совета Европейского союза от 1-2 октября (EUCO 13/20), ЕС задействует свои инструменты и регуляторную мощь, чтобы помочь сформировать глобальные правила и стандарты», – сказано в проекте резолюции.

В частности, следует усилить возможности ЕС для самозащиты от киберугроз, создания безопасной сферы коммуникаций, особенно с помощью квантового шифрования, и гарантировать доступ к данным в юридических и правоохранных целях, говорится в документе (*ЕС готов узаконить доступ спецслужб к зашифрованной переписке в мессенджерах – документ // <https://d-russia.ru/es-gotov-uzakonit-dostup-specsluzhb-k-shifrovannoj-perepiske-v-messendzherah-dokument.html>. – 2020. – 09.11*).

**Центр правительственной связи Великобритании (Government Communications Headquarter, GCHQ) начал «наступательную» кибероперацию для блокировки пропаганды против вакцинации, распространяемой онлайн «враждебными государствами».**

Среди «враждебных государств» упомянута по имени только наша страна.

«Эта инициатива GCHQ, собирающей по всему миру информацию с целью идентифицировать и срывать угрозы для Великобритании, является попыткой противостоять дезинформационным действиям, связанным с Россией, – говорится в статье. – В ситуации, когда близится появление надёжной вакцины от коронавируса, правительство Британии считает блокировку недостоверной информации, связанной с иммунизацией, своим высшим приоритетом».

GCHQ поручено зачистить Интернет и, в частности, социальные сети от противников вакцинации. Речь об уничтожении созданного «враждебными государствами» контента и «лишении связи» ответственных за его распространение.

GCHQ, главная в Британии организация по части кибершпионажа, наряду с другими спецслужбами США, Великобритании, Австралии, Канады и Новой Зеландии входит в разведывательный альянс «Пять глаз» (*Вика Рябова Британская спецслужба начинает кибервойну с агитацией*



*против вакцинирования – СМИ // <https://d-russia.ru/britanskaja-specsluzhba-nachinaet-kibervojnu-s-agitaciej-protiv-vakcinirovanija-smi.html>. – 2020. – 09.11).*

### **Опыт регулирования информационного пространства в Иране.**

После Исламской революции 1979 года религия в Иране стала основой всех сфер жизни, в том числе правовой системы страны. Право в Иране представляет собой сочетание романо-германской правовой системы и шариата. Роль принципов ислама в качестве основы правовой системы страны гарантирована Конституцией Ирана, принятой в 1979 году. Согласно статье 4 Конституции «все гражданские, уголовные, финансовые, экономические, административные, культурные, военные, политические нормы и любые другие законы должны основываться на принципах ислама. Эти принципы главенствуют над всеми нормами Конституции и другими нормативными правовыми актами». Преступления против бога и государства, в том числе совершённые с использованием Интернета, считаются самыми тяжкими.

Главой судебной системы Ирана является муджтахид (исламский богослов, достигший совершенства в знании и толковании Корана). В его обязанности входит надзор за тем, чтобы Верховный суд и вообще судебная система действовали согласно нормам шариата, а порядок согласования законопроектов и назначение должностных лиц также соответствовали религиозному закону. Глава судебной системы, проконсультировавшись с судьями Верховного суда, назначает председателя Верховного суда и генерального прокурора, предлагает главе государства кандидата на пост министра юстиции, а также выбирает шесть из 12 членов Совета стражей Конституции Ирана (специальный орган власти Ирана, осуществляющий надзор за исполнением Конституции всеми государственными органами).

Верховный суд осуществляет контроль над системой нижестоящих судов и следит за единообразием юридической процедуры, он также является последней апелляционной инстанцией. Судьёй Верховного суда, так же как генеральным прокурором, может стать только муджтахид.

*Модель регулирования Интернета в Иране представляет собой разновидность ближневосточной модели* – вследствие существенной роли религиозного фактора при принятии решений о привлечении к ответственности пользователей Интернета и о правовом регулировании Интернета, в том числе при определении критериев для блокировки интернет-ресурсов.

Однако из-за широкого развития информационных технологий и растущей популярности Интернета среди граждан Ирана в настоящее время государство ищет баланс между традиционными и современными принципами организационно-правового регулирования законодательства применительно к Интернету.

Согласно Конституции «средства массовой информации должны служить распространению исламской культуры в процессе развития Исламской революции, используя конструктивное столкновение различных мнений и идей, решительно воздерживаться от распространения деструктивных сил и антиисламских явлений».

Поэтому высшие государственные и религиозные лидеры Ирана уделяют большое внимание проблемам информационной политики и информационной безопасности государства не только в СМИ, но и в киберпространстве, полагая, что в настоящее время против Ирана со стороны западных государств ведется жёсткая информационная война.

### **Статистические сведения, характеризующие особенности использования Интернета гражданами Ирана. Блокировка запрещенных онлайн-платформ**

Среди стран юго-западной Азии Иран одним из первых подключился к Интернету. В январе 1992 года первая выделенная линия соединила Иран с европейскими университетами в Европейской сети академических исследований (EARN). Первоначально Интернет был доступен только высшим государственным чиновникам, студентам и сотрудникам научно-исследовательских центров. Каких-либо ограничений для пользователей практически не было.

Первым провайдером, предоставлявшим доступ к Сети широкому кругу пользователей, стала государственная компания Data Communication Company of Iran (DCI), работающая до сих пор. Помимо доминирующей DCI популярны провайдеры CompuServe, IRNET (Information and Communication Network of Iran) и Aradana. Ведущий хостинг-провайдер – Neda Rayaneh.

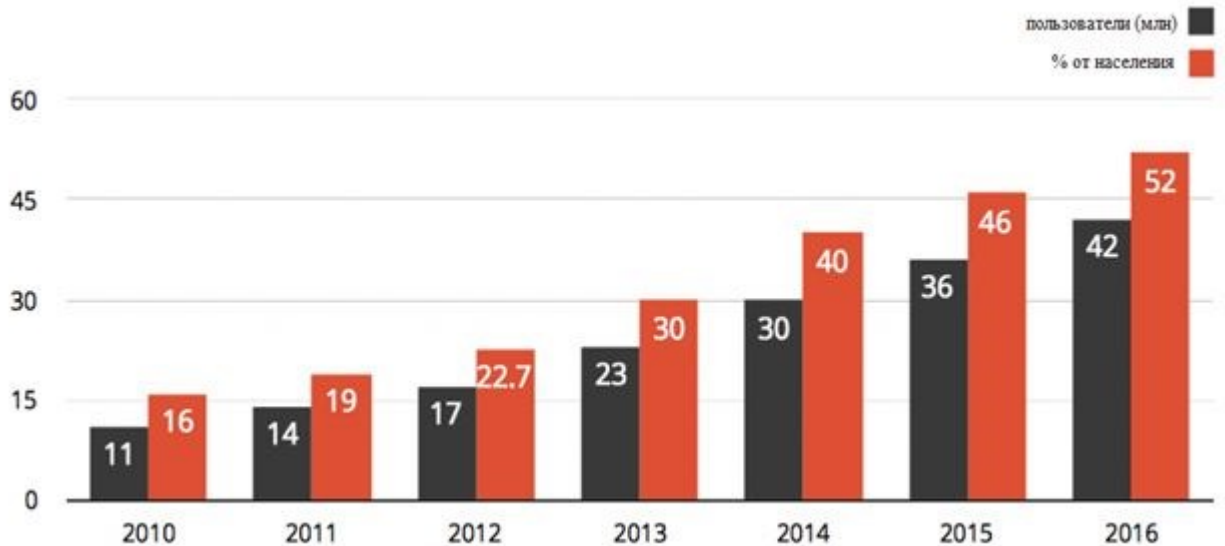
Существенное развитие Интернет в Иране получил в 1997 году благодаря реформам президента Хатами. С 1994 по 1999 годы число пользователей в Иране выросло с 10 тысяч до 100 тысяч человек, при этом Тегеран существенно опережал другие регионы.

На сегодняшний день общее количество пользователей сети «Интернет» в Иране превышает 50 миллионов при населении почти в 83 миллиона человек. В Иране насчитывается примерно 140 операторов связи, обеспечивающих доступ к Интернету. Большинство из них частные. Операторы лицензируются государством. Чтобы получить лицензию интернет-провайдера, заявитель должен быть гражданином Ирана, исповедовать официальную религию страны и не состоять в каких-либо незаконных организациях.

В Иране популярны интернет-кафе, до 2012 года их посетители могли выходить в Интернет анонимно. В 2012 году был принят закон «О деятельности интернет-кафе», согласно которому посетители должны предоставить удостоверение личности с фотографией и дать согласие быть снятыми на камеры видеонаблюдения. Закон обязывает владельцев кафе сохранять эти видеозаписи, как и историю просмотра сайтов посетителями кафе, в течение шести месяцев. Законом «О деятельности интернет-кафе»

установлено, что граждане, желающие открыть интернет-кафе, должны быть женаты или замужем.

В 2009 году иранцы в среднем проводили 188 минут в день у телевизора и около 48 минут в Интернете, к 2017 году на телевизор приходилось 157 минут, а на Интернет – 164 минуты, по данным fararu.com.



Темпы роста интернет-аудитории в Иране в период с 2010 по 2016 гг. Источник: fararu.com

Главная проблема для иранских пользователей состоит в низкой скорости соединения. Поэтому самыми популярными в стране становились онлайн-сервисы, не требующие большой скорости для нормального функционирования. Отсюда широкая популярность мессенджера Telegram (как до его блокировки в 2017 году, так и после), который в отличие от WhatsApp и Viber работоспособен при медленном соединении. Аналогичным образом приобрел популярность на территории Ирана и Instagram (также заблокирован на территории Ирана с 2017 года), второй по популярности после Telegram. Все конкурирующие с Instagram приложения нуждались в лучшем качестве соединения. При этом главные конкуренты Instagram – Twitter, Facebook и «ВКонтакте» – заблокированы были значительно раньше, в 2009 году.

Широкая популярность в Иране названных сервисов также обусловлена возрастом аудитории этих платформ: половина интернет-пользователей – люди 18-24 лет.

Качество проводного доступа в Иране существенно уступает возможностям мобильного Интернета, поэтому в большинстве случаев люди выходят Интернет не с компьютеров, а со смартфонов, что также обусловило популярность Telegram и Instagram.

Для Telegram Иран – первая страна по числу пользователей: 40 миллионов. В Instagram зарегистрированы 24 миллиона иранцев (данные на февраль 2018 года, уже после блокировки Instagram на территории Ирана).

Пользователи обходят ограничения с помощью VPN-сервисов. Государство рассматривает их как угрозу, препятствующую блокировке порносайтов, анонимайзеров, сайтов для гомосексуалистов, политических сайтов, сайтов о правах женщин и многих других, которые считаются незаконными.

Согласно исследованиям Тегеранского университета, после блокировки посещение каналов на персидском языке в Telegram только в первые дни упало с 2,4 миллиарда заходов в день до 850 миллионов, потом начался рост, и через три недели показатель достиг значения 1,6 миллиарда.

В ответ органы власти попытались заблокировать сервисы для обхода блокировок. В результате вышли из строя ключевые элементы интернет-инфраструктуры: центры обработки данных, хостинги, облачные хранилища. Это привело к сбою в работе иранских коммерческих структур, сервисов и сайтов.

### **Общие сведения о законодательном регулировании сети Интернет.**

#### **Контроль и надзор за использованием Интернета в Иране**

Надзор за использованием Интернета в Иране значительно усилился во времена президента Махмуда Ахмадинежада (шестой президент Ирана, занимавший пост в 2005-2013 годах). Показательно были осуждены ряд лиц за преступления, совершенные ими в Интернете.

В этой связи следует отметить особенности привлечения к уголовной ответственности в Иране. Уголовный Кодекс Ирана является основным и наиболее важным источником уголовного права. Он представляет собой кодифицированный нормативный правовой акт и состоит из пяти отдельных книг, принятых в разные периоды времени.

Принципы уголовного наказания по шариату кодифицированы и закреплены также в Уголовном кодексе Ирана. ***Можно выделить четыре основных принципа, применяющихся к разным категориям преступлений:***

«Ходуд (или Хадд)» – наказание, степень которого определяется только по шариату и исключает возможность применения других источников; это наказание устанавливается за самые тяжкие преступления против Аллаха.

«Кесас» – наказание по принципу возмездия («око за око»); оно сопутствует тяжким преступлениям против «своего ближнего».

«Диа» – денежный штраф («деньги за кровь»), выплачиваемый преступником родственникам пострадавшего, сумма штрафа колеблется в зависимости от тяжести причинённого вреда, от увечья до убийства.

«Таазират» – наказание, мера которого не может быть определена на основе шариата и устанавливается судьей в соответствии с ещё одним источником права под названием «акль». Это может быть лишение свободы, штраф или розги.

В Иране узаконена смертная казнь. Она может применяться в качестве наказания за убийство, изнасилование, соращение несовершеннолетнего, содомию, торговлю наркотиками, вооружённое ограбление, похищение

человека, терроризм и государственную измену. Смертный приговор приводится в исполнение несколькими методами: повешение, расстрел, обезглавливание, сбрасывание с большой высоты.

Согласно Уголовному кодексу Ирана, преступлением считается публикация в Интернете любого материала, оскорбляющего исламскую доктрину, ценности иранской революции, мысли имама Хомейни, Конституцию Ирана, ставящего под угрозу национальное единство страны, создающего положительный имидж незаконных организаций, разглашающего секретную информацию, содержащего рекламу курения, обвиняющего или оскорбляющего чиновников.

В августе 2014 года был приговорён к смертной казни иранский блогер Сохейль Араби – за то, что он оскорбил пророка Мухаммеда в Facebook.

Одновременно система регулирования киберпространства Ирана представляет собой отлаженный механизм упорядоченного функционирования ряда государственных и негосударственных структур.

Главным органом в стране, отвечающим за сферу онлайн-коммуникаций, является Высший совет по киберпространству, исполнительный политический орган Ирана, основанный в соответствии со статьей 176 Конституции, в который кроме президента Ирана входят представители Корпуса стражей Исламской революции (иранское военно-политическое формирование, созданное в 1979 году из военизированных отрядов исламских революционных комитетов, сторонников лидера иранских шиитов великого аятоллы Хомейни). Высший совет по киберпространству создан в 2012 году с целью предотвращения киберугроз и координации политики в киберпространстве.

Важнейшими задачами совета являются политика фильтрации Интернета и координация развития интернет-технологий. Совет действует под непосредственным руководством лидера Ирана Али Хаменеи, а в его состав входят главы служб разведки и безопасности, судебной власти, государственного радио и телевидения и др. представители органов власти).

Высшему совету по киберпространству подчинены несколько уполномоченных ведомств.

Национальный центр киберпространства. Отвечает за мониторинг технологических и политических нововведений как в глобальном киберпространстве, так и в пределах страны. Контролирует исполнение указов Высшего совета по киберпространству.

Комитет по определению случаев криминального контента. Отвечает за фильтрацию и блокировку интернет-контента. Создает списки сайтов, которые нарушают общественную мораль, противоречат исламу, угрожают национальной безопасности, критикуют государственных служащих либо организации, пропагандируют инструменты обхода блокировки.

Киберполиция Ирана. Является отделением иранского полицейского управления для борьбы с такими киберпреступлениями, как фишинг и пр.

Киберармия Ирана. Представляет собой группу хакеров, атакующих оппозиционные и антиисламские сайты.

Министерство информационных и телекоммуникационных технологий. Отвечает за фильтрацию источников информации из списков, которые подготавливаются Комитетом по определению случаев криминального контента. Регулирует процесс запуска Национальной информационной сети. Управляет национальным сегментом Интернета и всеми коммуникационными инфраструктурами, что, в свою очередь, непосредственно влияет на систему мониторинга и фильтрации контента.

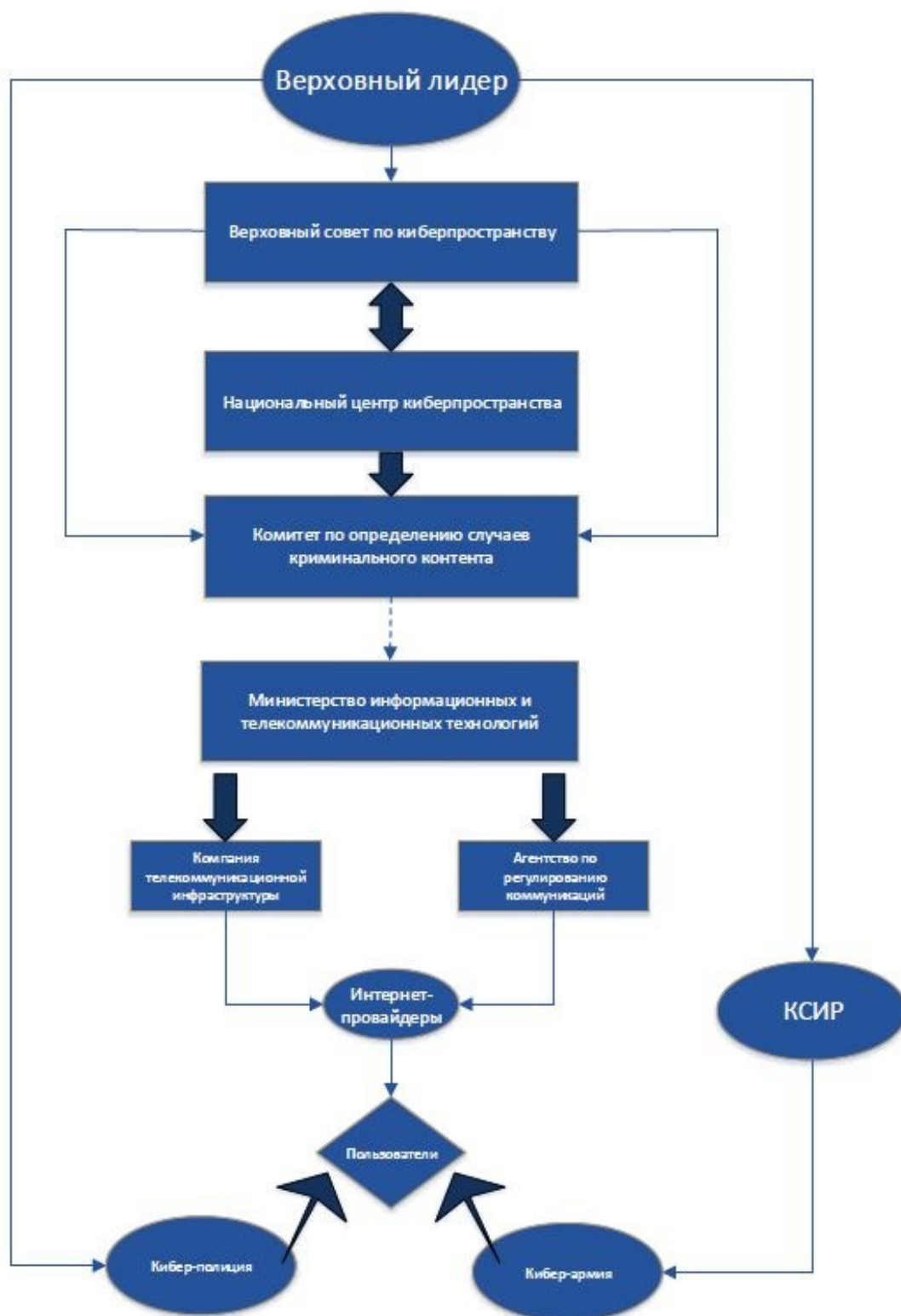
В ведении Министерства информационных и телекоммуникационных технологий находятся следующие структуры.

Компания телекоммуникационной инфраструктуры, обеспечивающая инфраструктуру для национальной сети передачи данных.

Агентство по регулированию коммуникаций. Занимается лицензированием телекоммуникационных технологий. Предоставляет лицензии интернет-провайдерам и отвечает за контроль качества интернет-сервисов. Отслеживает исполнение поручений правительства по фильтрации интернет-контента.

Особую роль в стране играет Корпус стражей исламской революции. Его вовлеченность в сферу информационно-телекоммуникационной инфраструктуры обосновывается необходимостью защиты страны от идеологического вмешательства. Вследствие этого приобрел популярность термин «культурное вторжение», означающий проникновение западной культуры в Иран с целью разрушения исламских ценностей.

В 2012 году Высшему совету по киберпространству было поручено сформулировать политику Ирана в отношении Интернета, а также разработать планы его регулирования в соответствии с Конституцией. Высший совет по киберпространству издал доктрину «Официальная система идентификации в киберпространстве», согласно которой государству необходимо предоставить полномочия по идентификации интернет-пользователей. Другими нормативными правовыми актами вопрос регулирования персональных данных на территории Ирана не урегулирован. Единый кодифицированный нормативный правовой акт в области регулирования персональных данных в Иране отсутствует.



Организационная структура органов власти Ирана, регулирующих сеть Интернет  
Сложность обеспечения эффективных мер законодательного регулирования Интернета в Иране определяется быстрым развитием интернет-технологий и появлением новых видов информационных угроз.

Особое значение приобретают вопросы квалификации ответственности за нарушения законодательства Ирана с использованием Интернета. Так, статья 500 Уголовного кодекса гласит: «Любой, кто занимается любого рода пропагандой против Исламской республики Иран или поддерживает оппозиционные группы и ассоциации, должен быть приговорён к лишению свободы на срок от трёх месяцев до одного года». Однако в законодательстве не содержится конкретного определения термина «пропаганда», что даёт судьям широкие полномочия для квалификации сообщений пользователей Интернета как пропаганды.

В 2009 году в Иране принят закон «О компьютерных преступлениях», который разрешает правительству фильтровать контент, противоречащий «порядочности и общественной нравственности».

Как следствие, в Иране занялись исследованием правового регулирования распространения информации в Facebook и Twitter, в том числе для противодействия организации массовых беспорядков. В целях обеспечения государственной безопасности в конце мая 2009 года указанные выше социальные сети на территории Ирана были заблокированы.

Доступ к Википедии для иранских пользователей был закрыт ещё в декабре 2006 года, одновременно с запретом других популярных сайтов, таких, как YouTube и IMDb. В Иране запрещены многие сайты с антиисламским содержанием и оппозиционные сайты. Заблокированы версии сайтов некоторых иностранных СМИ на персидском языке, в то время как их англоязычные версии не блокируются.

### **Подавление массовых протестов в Иране путём ограничения доступа к Интернету**

Действующие в Иране ограничения сложились ввиду внутривнутриполитической ситуации в государстве.

В протестах, проходивших в арабских странах в 2010-2011 годах (т.н. «арабская весна»), в том числе в Иране, протестующие использовали интернет-платформы для организации массовых акций. В ответ власти Ирана на несколько дней ограничили гражданам доступ к Интернету. Высший совет по киберпространству был создан после этих событий.

Также в указанный период получил развитие проект «Национальная информационная сеть Ирана». Это попытка создать на территории Ирана национальный безопасный Интернет, отвечающего критериям «исламского контента», что означает блокировку или фильтрацию информации по политическим, культурным и религиозным критериям.

В августе 2016 года завершена первая фаза проекта, в феврале 2017 года – вторая фаза, а 16 июля 2017 года завершился третий этап и состоялся запуск национальной сети.

Первая фаза предполагала внедрение инфраструктуры и отделение национального сегмента Сети. Запуск второй фазы включал миграцию онлайн-сервисов на хостинг внутри Ирана. На третьем этапе реализован



доступ ко всем электронным государственным сервисам посредством национальной информационной сети.

В ноябре 2019 года после массовых протестов, вызванных повышением цен на топливо (на 200 % за одну ночь и в преддверии зимы), руководство Ирана ограничило доступ к Интернету на территории страны с 16 ноября по 25 ноября. Блокировку местных онлайн-сервисов это не повлекло.

Блокировки нанесли существенный ущерб деятельности многих юридических лиц, в связи с чем министр информационно-коммуникационных технологий страны Мохаммад Джавад Азари Джахроми заявил о необходимости компенсировать ряду интернет-компаний финансовые потери.

### Заклучение

Государственное регулирование Интернет в Иране обусловлено приоритетной ролью информационно-телекоммуникационной сферы во внутренней политике. При регулировании сделан акцент на соблюдение принципов ислама, т.к. право в Иране представляет собой сочетание романо-германской правовой системы и шариата.

Власти Ирана исходят из того, что доступ граждан к Twitter, Facebook, Instagram, Telegram и другим социальным онлайн-сервисам будет способствовать распространению в стране недопустимого контента. Эти сервисы в Иране заблокированы.

Ограничения привели к быстрому освоению пользователями VPN-сервисов.

Для кардинального решения проблем, связанных с регулированием Интернет, в стране реализован проект «Национальная информационная сеть Ирана». В стране создана отдельная от Интернет интранет-сеть.

Исламская Республика Иран выстроила масштабный, активно развивающийся механизм регулирования интернет-пространства с учётом национальных культурных традиций и, что важнее, идеологических особенностей информационной политики государства (*Александр Федотов Опыт регулирования информационного пространства в Иране // <https://d-russia.ru/opyt-regulirovanija-informacionnogo-prostranstva-v-irane.html>. – 2020. – 05.11).*

**Крупные соцмедиакомпании – Facebook, Instagram, Twitter, Periscope, YouTube и TikTok – оштрафованы в Турции на 10 миллионов лир (1,18 миллиона долларов) каждая за неисполнение требований нового закона.**

Закон, вступивший в силу в октябре, обязывает интернет-платформы с ежедневной пользовательской аудиторией более миллиона человек назначать своих представителей для взаимодействия с турецкими судами. Также законом введено требование об удалении «оскорбительного» контента в течение 48 часов и хранении данных турецких пользователей на территории Турции.

Какие именно положения этого закона нарушили оштрафованные компании, не уточняется.

Как заявил председатель турецкого регулятора в сфере IT и коммуникаций, если оштрафованные компании не устранят нарушения, размер штрафа будет увеличен до 30 миллионов лир (3,5 миллиона долларов), их реклама будет заблокирована, а пропускная способность интернет-каналов для них будет уменьшена наполовину в течение пяти месяцев.

Компании-рецидивисты рискуют дожидаться уменьшения пропускной способности каналов до 10 % от стандартной.

Если же нарушения будут устранены, ограничения на трафик снимут, а штраф снизится на 75 % (*Вика Рябова Турция оштрафовала иностранные IT-сервисы за неисполнение национального законодательства // <https://d-russia.ru/turcija-oshtrafovala-inostrannye-it-servisy-za-neispolnenie-nacionalnogo-zakonodatelstva.html>. – 2020. – 05.11*).

## **Новітня бібліографія зарубіжних та вітчизняних досліджень з проблематики електронного урядування**

Анализ международной практики разработки и внедрения цифровых платформ в сфере публичного управления. *E-Management*. 2020. Т. 3. № 3. С. 34-44. Реализация задачи создания цифровой платформы полнофункциональной системы информационно-аналитического обеспечения управления на федеральном, региональном и муниципальном уровнях требует больших затрат ресурсов и серьезной экспертизы. В связи с этим предмет исследования – опыт и тенденции построения и эксплуатации цифровых платформ государственного и публичного управления. Цель работы состояла в обобщении международной практики создания, эксплуатации и развития цифровых платформ публичного управления. В рамках исследования проведен системный, контентный и сравнительный анализ различных источников: нормативно-правовых документов, научных работ, аналитических материалов ряда международных организаций и др. В статье представлены результаты исследования мирового опыта в области применения различных инструментов поддержки электронного правительства и сопровождения цифровых платформ управления. Приведено описание тенденций использования информационно-коммуникационных технологий поддержки государственного управления. Представлен перечень общих принципов функционирования цифровых платформ управления; приведены результаты анализа на соответствие этим принципам государственных цифровых платформ Европейского союза; выделены их отличительные свойства. На основе результатов анализа и доступных исследований по проблематике развития и продвижения цифровых платформ управления сформированы предложения и направления развития, которые могут способствовать ускорению распространения цифровой трансформации госуправления. Результаты исследования могут быть применены для выявления потенциала существующей платформы, ее сильных и слабых сторон, в том числе в контексте возможностей развития процесса цифровой трансформации управления, а также эффективного продвижения в направлении формирования цифровой платформы государственного/публичного управления.

Букуева, А. О. Международный опыт формирования и развития государственной политики в сфере оказания электронных государственных услуг. *Вестник Академии государственного управления при Президенте Кыргызской Республики*. 2020. № 27. С. 110-117. Во многих странах мира, таких как, Дания, Англия, США, Япония, Сингапур разработаны и реализуются стратегии информационного развития как общества в целом, так и отдельных сфер деятельности. Однако, на сегодня нет унифицированного шаблона, который отвечал бы всем условиям и решениям задачи формирования электронного правительства. Каждая страна обладает уникальным сочетанием обстоятельств, приоритетов, наличных ресурсов, которые используются при реализации поставленной задачи. Но, тем не менее, в процессе организации электронного правительства подавляющее большинство стран мира делают упор на электронный доступ к основным общедоступным услугам. Проведенное исследование зарубежного опыта стран-лидеров по электронному правительству представляется крайне актуальным для их возможного практического воплощения при преобразовании государственного управления в Кыргызской Республике. На основе проведенного исследования в статье рассмотрен зарубежный опыт стран-лидеров по

развитию электронных государственных услуг с учетом актуальных тенденций развития электронного правительства в мире, показан уровень развития системы оказания электронных государственных услуг зарубежных стран на разных этапах развития общества.

*Бурый, А. С.* Совершенствование государственных информационных систем как тренд цифрового общества. *Правовая информатика*. 2020. № 3. С. 9-28. Цель работы: совершенствование концептуально-методической базы информационно-коммуникационных технологий для формирования единого информационного пространства в государственном секторе управления. Метод: комплексирование системного и сравнительного анализа на основе статистических выводов и приемов функционально-логической классификации. Результаты: на основе анализа хода реализации стратегии государства на построение цифрового общества, направленного как на повышение качества предоставляемых гражданам электронных услуг, так и на рост эффективности коммуникационных процессов органов государственного управления, предлагается комплексное использование перспективных информационно-коммуникационных технологий и системного подхода при формировании требований к государственным информационным системам и к разработке их правового, методического, информационного, программного и модельно-алгоритмического обеспечения, опираясь на концепции онтологического инжиниринга, потенциал методов интеллектуального анализа данных, технологии облачных вычислений и социальных коммуникаций.

*Куаналиев, А. А.* Цифровизация государственного управления -залог успешного развития государственного сектора. *Научный результат. Технологии бизнеса и сервиса*. 2020. Т. 6. № 3. С. 35-46. Вопрос эффективности государственной власти возник практически с момента ее возникновения, при этом время от времени актуальность данного вопроса обновлялась в силу сравнения с другими более успешными странами. В конце XX века данное направление получило второе дыхание, практически параллельно со вторым рождением актуальности проблемы эффективности государства началась эпоха цифровизации. За прошедшие двадцать лет в цифровизации сделаны огромные шаги, сравнимые с технологической революцией XVIII-XIX веков. Более того, сегодня мы живем в эпоху индустриализации 4.0. Таким образом, два понятия: эффективность государственного сектора и цифровизация, плотно переплелись между собой. Логично предположить, что между ними имеется корреляция. В статье методом математического анализа (методом Крамера) проверено и подтверждено предположение о наличии такой связи, в результате выявлен высокий индекс корреляции. Для проведения анализа в качестве показателя эффективности государственного сектора выбран индекс процветания Института Legatum (The Legatum Prosperity Index), а для определения уровня развития цифровизации государственного сектора той или иной страны Индекс развития электронного правительства (The UN Global E-Government Development Index). Оба индекса являются комплексными показателями, отражающими соответствующие уровни развития. Они начали разрабатываться в XX веке, в основу берутся статистические данные, полученные из Организации Объединённых Наций, Всемирного банка, Организации экономического сотрудничества и развития, Всемирной Торговой организации, Gallup, Economist Intelligence Unit, IDC, Pyramid Research и других институтов.

*Маннанова, Ш. Г., Шоахмедова, Н.* Цифровая трансформация в сельском хозяйстве (agtech) в Республике Узбекистан. *Экономика и бизнес: теория и*

*практика.* 2020. № 10-2 (68). С. 44-46. В данній статтє рассматриваются актуальные вопросы цифровизации сельского хозяйства в Республике Узбекистан, а также рассмотрены основные направления постановления Президента «О мерах по широкому внедрению цифровой экономики и электронного правительства». Рассмотрены вопросы подготовки высококвалифицированных кадров для развития цифровой экономики в Республике Узбекистан.

*Мельничук, Н. Ю.* Електронне урядування: сучасний стан та перспективи застосування у бюджетній сфері. *Збірник наукових праць Національного авіаційного університету «Проблеми системного підходу в економіці».* Випуск 5(73). 2019. С. 97–105. У статті досліджено окремі історичні аспекти розвитку електронного урядування в Україні. Виокремлено напрями розвитку електронного урядування в Україні, досліджено головні його складники. Проаналізовано рейтинг розвитку електронного урядування в окремих країнах світу та в Україні. З'ясовано, що система електронного бюджету в Україні на загальнодержавному та місцевому рівнях не використовується і не є дослідженою. Запропоновано ввести у науковий обіг економічне поняття «е-бюджет» під яким запропоновано розуміти систему організації державного управління, яка передбачає взаємодію органів державної влади між собою, з органами місцевого самоврядування і населенням незалежно від місця їх розташування, з використанням інтегрованих інформаційних технологій з метою підвищення ефективності формування й використання бюджетних коштів і забезпечення результативності бюджетного менеджменту в системі державного регулювання. Перераховано перспективні напрями впровадження системи е-бюджету в Україні. Обґрунтовано, що її запровадження сприятиме прозорості та відкритості діяльності органів державної влади та органів місцевого самоврядування перед зовнішніми користувачами.

*Романчук, О. З.* Розширене розуміння електронного урядування у сучасній правовій системі. *Юридичний бюлетень.* Випуск 14. 2020. С. 69-75. Технологічні ресурси весь час розвиваються, знаходячи все ширшу сферу апробації, серед них – оновлення форми управління у публічно-владній сфері. Цифровий уряд розпочав значні та тривалі зміни у способі життя людей і їхній взаємодії між собою та громадськими інституціями. Інформаційні технології та інновації впливають на суспільний сектор і змінюють повсякденне життя людей. Проаналізовано чинне нормативне законодавство, яке визначає понятійно-категоріальний апарат електронного урядування. Вказано, що поняття, яке детерміновано в законодавстві, є застарілим, оскільки не відображає сучасних тенденцій і має низку недоліків. По-перше, воно містить декларативні широкі категорії, опосередковано визначає основну сутність поняття – послуги надаються через інформаційні-комунікативні технології. По-друге, незрозуміло, що мав на увазі нормотворець, визначаючи «для формування нового типу держави». Говорити про новий тип держави в широкому розумінні не зовсім правильно, оскільки, незважаючи на впровадження електронної комунікації, держава продовжує мати такий самий тип виробництва, традиційні способи отримання прибутку, користування власністю та традиційні форми надання послуг. По-третє, акцентується увага на задоволенні потреб громадян. Вказане не є доречним, оскільки електронне урядування сьогодні – це система, яка характеризує дуже широку сферу відносин органів публічної влади та фізичних осіб (до того ж, це не завжди громадяни, це можуть бути іноземці, особи без громадянства, біженці, оскільки для них також працюють широкі сервісні послуги), а також юридичних осіб, тому що налагодження відносин влади та бізнесу також входить до новітньої системи урядування. Доведено, що сьогодні електронне урядування слід

розуміти масштабніше, ніж надання електронних послуг технічними засобами, оскільки урядування набагато розширило сферу застосування шляхом включення участі всіх зацікавлених суб'єктів та участі в управлінні. Акцентуємо на тенденції до розширення системи електронного урядування, що передбачає не тільки збільшення сфер і видів послуг, але й суб'єктів взаємодії. Нині електронне урядування вийшло за територіальні межі держави. Колективні глобальні зусилля зосереджені на більшому визнанні інституційних зв'язків між економічними, соціальними й екологічними аспектами сталого розвитку, тому електронне урядування використовується не тільки на національному та регіональному рівні, але і як ресурс у досягненні вищих життєвих рівнів для майбутніх поколінь у всьому світі. Така міжнародна сфера проявляється принаймні в тому, що електронне урядування покращує інформування обговорень міждержавних органів; сприяє боротьбі з глобальними катастрофами та кіберзлочинністю.

*Тимошенко, А. А.* Онлайн-сервиси сайта министерства внутренних дел Республики Беларусь. *Вопросы науки и образования*. 2020. № 12 (96). С. 4-7. В статье с позиции социальной значимости анализируется текущее положение справочных онлайн-сервисов, предоставляемых на сайте Министерства внутренних дел Республики Беларусь. Рассматривается работа каждого сервиса, на основании этого дается авторская оценка всей системы онлайн-сервисов.

*Щербакова, К. Ю.* Розвиток електронного урядування в Україні в контексті зарубіжного досвіду. *Традиції та інновації розвитку приватного права в Україні: освітній вимір* : матеріали VIII Всеукраїнської науковопрактичної конференції (м. Полтава, 7 червня 2019 р.). – Полтава : ПУЕТ, 2020. – С. 184-187.