



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. Кушнарьова, 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

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 10 (84)

(огляд матеріалів ЗМІ за 1 – 31 жовтня 2020 р.)

Зміст

Анонс.....	4
Офіційна інформація.....	7
Регіональні ініціативи.....	19
Експертний погляд.....	24
Блоги та соціальні мережі	31
Зарубіжний досвід.....	42
Новітня бібліографія зарубіжних та вітчизняних досліджень з проблематики електронного урядування.....	73

Анонс

30 жовтня – 1 листопада 2020 р. (Київ)

Hack for Locals 2.0: «Безпечні спільноти» (Safer Communities Hackathon).

Міністерство цифрової трансформації України спільно із програмою ООН із відновлення та розбудови миру запрошують взяти участь у хакатоні Hack for Locals 2.0: «Безпечні спільноти» (Safer Communities Hackathon).

Об'єднання небайдужих учасників з усієї України – розробників, дизайнерів, представників громад, управлінців, активістів та ентузіастів громадянського суспільства, надавачів послуг з безпеки, підприємців і маркетологів для плідної співпраці та пошуку рішень, які сприятимуть побудові більш «розумних», сильних, безпечних і згуртованих спільнот.

Три найкращі проекти отримують грант на реалізацію ідей від Програми ООН із відновлення та розбудови миру (сума гранту складає від \$3 000 до \$30 000 залежно від ідеї та географії проекту), підтримку в складанні грантової заявки, менторську допомогу від організаторів та інші цінні призи від партнерів.

Ідея проекту має відповідати одному з напрямів:

- Цифрова безпека та цифрова грамотність.
- Інклюзивні послуги з безпеки для кожного.
- Координація діяльності між різними надавачами послуг з безпеки та громадами.

- Реагування на кризи та можливості раннього попередження/сповіщення (як об'єднати громадян, представників влади та надавачів послуг з безпеки на місцевому рівні в разі надзвичайної ситуації або загрози, для того, щоб провести необхідні превентивні заходи та зробити спільні дії швидшими та ефективнішими).

- Громадська безпека на основі фактичних даних (як використовувати дані з відкритого доступу (open data) для спільної користі).

Зареєструватися можна hackforlocals.org.

Hack for Locals 2.0: «Безпечні спільноти» (Safer Communities Hackathon) організований в межах Програми ООН із відновлення та розбудови миру у співпраці з Міністерством цифрової трансформації України, Платформою кар'єрного розвитку Happy Monday та агентством інновацій Center42, за фінансової підтримки Європейського Союзу та урядів Данії, Канади, Нідерландів, Швейцарії та Швеції.

Програму ООН із відновлення та розбудови миру реалізують чотири агентства ООН: Програма розвитку ООН (ПРООН), Структура ООН з питань гендерної рівності та розширення прав і можливостей жінок (ООН Жінки), Фонд ООН у галузі народонаселення (UNFPA) і Продовольча та сільськогосподарська організація ООН (ФАО).

Програму підтримують тринадцять міжнародних партнерів: Європейський Союз, Європейський інвестиційний банк, Посольство США в Україні, а також уряди Великої Британії, Данії, Канади, Нідерландів, Німеччини, Норвегії, Польщі, Швейцарії, Швеції та Японії (*Мінцифри та ПРООН оголошують хакатон для розвитку громад Hack for Locals 2.0 // <https://thedigital.gov.ua/news/mintsifri-ta-proon-ogoloshuyut-khakaton-dlya-rozvitku-gromad-hack-for-locals-20>*).

18–19 Ноября, 2020 г. (Санкт-Петербург, РФ)

Седьмая международная конференция «Электронное управление и открытое общество: вызовы Евразии» (Electronic Governance and Open Society: Challenges in Eurasia) EGOSE-2020

Организаторы: Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО» (Университет ИТМО) и Северо-Западный Институт Управления Российской академии народного хозяйства и государственной службы при Президенте РФ (СЗИУ РАНХиГС)

Важная задача конференции – способствовать формированию в Евразийском пространстве международного сообщества специалистов, ведущих исследования и разработки в области технологий информационного общества, электронного правительства, электронного управления и электронной демократии. Конференция способствуют изучению зарубежного опыта и развитию международного сотрудничества в данной области. С 2014 г. конференция стала международной и единственной англоязычной конференцией в России по заявленной тематике.

По причине пандемии COVID-19, в этот раз конференция будет проводится в смешанном формате: Очном, для тех кто желает и может приехать в Санкт-Петербург и в формате ZOOM-конференции для тех, кто предпочтет участвовать дистанционно.

Программный комитет EGOSE-2020 приглашает авторов предлагать к презентации и публикации оригинальные работы *по следующим тематикам:*

- Электронное управление и Евразийская интеграция
- Перспективы и проблемы «Открытого правительства»
- Информационное общество и электронное управление
- Электронное правительство, ориентированное на граждан
- Создание умных городов
- Умный город, Умный гражданин и качество жизни
- Электронное управление и моделирование политик
- Электронное участие и инициативное бюджетирование
- Социальные сети: инструменты анализа, участие и эффекты
- Практические примеры, эффекты и тенденции электронных трансформаций в государственном и муниципальном управлении

Робочий язык конференції – англійський.

Рецензування і оцінка поданих на конференцію статей здійснюється міжнародним програмним комітетом по стандартній процедурі подвійного сліпого рецензування (мінімум три рецензії) для забезпечення високого наукового рівня конференції і уникнення конфлікту інтересів.

Публікація: Подані і успішно пройшли процедуру рецензування статті будуть опубліковані в збірці Communications in Computer and Information Science (CCIS) видавництва Springer, індексованої в Scopus і інших індексах при умові оплати реєстраційного внеску і презентації статті на конференції, як мінімум, одним із авторів. К публікації приймається не більше двох статей одного автора.

Місце проведення конференції: Санкт-Петербург, ул.Ломоносова д.9. Університет ІТМО (<http://egov-conf.ifmo.ru/rus.html>).

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) 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

Кабинет министров опубликовал распоряжение о возобновлении системы электронного декларирования. Работа системы была заблокирована решением Конституционного суда Украины. Распоряжение правительства было принято 29 октября.

Правительство поручило Национальному агентству по предотвращению коррупции (НАПК) обеспечить открытый круглосуточный доступ к публичной части Единого госреестра деклараций.

Также НАПК должно обеспечить проведение специальных проверок согласно требованиям закона «О предотвращении коррупции».

В распоряжении также указано, что должны сделать госорганы и органы местного самоуправления для того, чтобы работа реестра и системы электронного декларирования возобновилась в полном объеме.

Однако в документе не указано, когда именно должно быть выполнено распоряжение правительства (*Распоряжение правительства о возобновлении системы электронного декларирования опубликовано // https://focus.ua/politics/466189-rasporiazhenie_pravitelstva_o_vozobnovlenii_sistemy_elektronnoho_deklarirovaniia_opublikovano. – 2020. – 29.10).*

Проект постанови «Про внесення змін до Порядку виготовлення і видачі посвідчень батьків багатодітної сім'ї та дитини з багатодітної сім'ї», за поданням Мінцифри та Мінсоцполітики сьогодні прийнято на засіданні Уряду.

Завдяки цьому рішенню, державні послуги стануть простішими та зручнішими для багатодітних сімей.

Відтепер такі сім'ї зможуть отримати посвідчення незалежно від місця реєстрації, та у будь-який зручний спосіб. На це у державних органів є 10 днів з моменту подачі заяви.

«Багатодітні сім'ї відтепер зможуть отримати посвідчення на підставі однієї заяви. Спростується і форма подачі: можна обрати зручний для себе спосіб – через інтернет, поштою або за особистим зверненням.», – зазначила **заступниця Міністра цифрової трансформації Людмила Рабчинська.**

Також відомості, необхідні для оформлення посвідчень батьків багатодітної сім'ї, можуть перевірятися у порядку електронної інформаційної взаємодії з державними електронними інформаційними ресурсами за допомогою засобів Єдиного державного вебпорталу електронних послуг.

Зазначений проект постанови розроблено Мінсоцполітики за ініціативи Мінцифри, Офісу реформ та SURGE, що фінансується Урядом Канади (*За ініціативою Мінцифри спрощені державні послуги для багатодітних сімей // <https://thedigital.gov.ua/news/za-initsiativoyu-mintsifri-sproshcheni-derzhavni-poslugi-dlya-bagatoditnikh-simey>. – 2020. – 28.10).*

Уряд затвердив Стратегію цифрової трансформації соціальної сфери, розроблену розроблену Мінсоцполітики разом з Мінцифрою.

«Прийняття Стратегії цифрової трансформації соціальної сфери – ще один крок до створення цифрової держави, в центрі якої людина. Наша мета – забезпечити найвищі стандарти надання адміністративних послуг та зробити їх доступними для всіх, особливо для соціально вразливих верств населення», – наголосив **Михайло Федоров, Віцепрем'єр-міністр – Міністр цифрової трансформації України**.

Цифрова трансформація дозволить усунути корупцію у соціальній сфері, а отже – підвищить доступ населення до соціальної підтримки та покращить якість надання адміністративних послуг соціального характеру. Впровадження стратегії також зробить соціальну сферу більш прозорою та оптимізує адміністративні видатки.

Серед пріоритетних цілей:

- Переведення послуг в онлайн
- Контроль операційних процесів у соцсфері
- Перехід на електронний документообіг у соціальній сфері
- Прозорий розподіл та контроль соціальних видатків у державі
- Інформування українців про їхні соціальні права, належні виплати та види соціальної підтримки

Для підвищення ефективності соціального захисту населення Мінцифра разом з Мінсоцполітики створює Єдину інформаційну систему соціальної сфери (ЄІССС), яка забезпечить оцифрування послуг та адміністрування всіх видів державної соціальної підтримки.

Стратегію буде реалізовано у два етапи: перший 2020–2021 роки та другий 2022–2023 роки (**Уряд затвердив Стратегію цифрової трансформації соціальної сфери, розроблену Мінсоцполітики разом з Мінцифрою // <https://thedigital.gov.ua/news/uryad-zatverdiv-strategiyu-cifrovoyi-transformaciyi-socialnoyi-sferi-rozroblenu-minsocpolitiki-razom-z-mincifroyu>. – 2020. – 28.10**).

Мінцифра зберігає бюджетні кошти та удосконалює документообіг в Секретаріаті Кабміну завдяки переводу проєктів актів Кабміну в електронну форму.

«Сьогодні відбулося перше засідання Уряду повністю онлайн, на якому прийняли постанову про можливість схвалювати нормативно-правові акти через електронний документообіг. Це останній крок до 100 % відмови від паперу в роботі Кабміну», – прокоментував **Віцепрем'єр-міністр – Міністр цифрової трансформації Михайло Федоров**.

Відтепер документи та постанови, винесені на Кабмін, будуть лише в електронній формі, без права вимагання їх дублювання на папері. Уряд схвалив відповідну постанову за ініціативи Мінцифри. Це ще один крок до створення цифрової держави.

Згідно із постановою електронна форма – первинна (основна) форма підготовки актів КМУ. Повний пакет супровідних документів формується та зберігається в електронній системі. Паперові примірники готуються як виключення або у випадках, передбачених законодавством. Крім того, електронна взаємодія органів виконавчої влади – тепер основний інструмент погодження актів.

Винятки становитимуть документи, що містять інформацію з обмеженим доступом.

Таке рішення дозволить значно скоротити бюджетні витрати, пов'язані зі створенням, проходженням та надсиланням паперових документів і пришвидшить прийняття рішень. А також удосконалив документообіг в СКМУ (*Мінцифра зберігає бюджетні кошти завдяки переводу проєктів актів Кабміну в електронну форму // <https://thedigital.gov.ua/news/mincifra-zberigaye-byudzhetni-koshti-zavdyaki-perevodu-proyektiv-aktiv-kabminu-v-elektronnu-formu>. – 2020. – 28.10).*

На заході зібралися провідні експерти FinTech галузі, банкіри та інвестори для того, щоб обговорити теми сучасної епохи цифрових фінансів: необанкінг, віддалену ідентифікацію, роль лідерства у діджитал трансформації тощо.

Людмила Рабчинська, заступник Міністра цифрової трансформації, розповіла про ICEI id.gov.ua та досягнення Мінцифри в галузі FinTech:

Мінцифра запустила ICEI id.gov.ua – універсальну платформу для е-ідентифікації та автентифікації користувачів, яка працює 24/7, має атестат КСЗІ, 4 підключених держреєстри та 196 клієнтів.

Відтепер завдяки 1 договору можна підключити всі способи ідентифікації. А це 53 схеми е-ідентифікації: 23 схеми КЕП та удосконалених підписів; 22 схеми BankID НБУ; 4 схеми на хмарних носіях; 3 схеми MobileID та можливість зберігати особистий ключ на ID-картці (тільки АЦСК МВС). Це означає, що банківські та небанківські установи зможуть легко встановити особу клієнта.

«Майбутнє за цифровізацією та онлайн-технологіями. Команда Мінцифри працює над тим, щоб комплексні й безпечні онлайн-сервіси для е-ідентифікації та автентифікації користувачів стали буденністю в фінансовій сфері. Наша задача – стрибок у майбутнє» (*Досягнення Мінцифри у галузі FinTech на конференції Digital Banking Conference & First FinTech Stand Up // <https://thedigital.gov.ua/news/dosyagnennya-mincifri-u-galuzi-fintech-na-konferenciyi-digital-banking-conference-first-fintech-stand>. – 2020. – 28.10).*

Міністерство цифрової трансформації пришвидшує запуск комплексної онлайн-послуги «Малютко в містах та областях України». Це особливо важливо під час пандемії, щоб мінімізувати контакт батьків немовлят з державними установами.

Для цього **перший заступник Міністра цифрової трансформації Олексій Вискуб** вже розпочав інспекцію українськими містами, щоб особисто проконтролювати та сприяти запуску послуги у пологових будинках в регіонах. Першою локацією став Житомир.

«З жовтня послуга «Малютко стала доступна онлайн на порталі Дія. Зараз її можуть замовити батьки новонароджених зі 139 населених пунктів у 15 областях. Реєстрація народження дитини ще ніколи не була такою швидкою, зручною та безпечною, що особливо важливо в умовах поширення Covid-19».

Щоб перевірити, як працює послуга, Олексій Вискуб відвідав Житомирський обласний перинатальний центр. Там вже запроваджено електронний медичний висновок про народження дитини. Його номер надсилається батькам в смс-повідомленні та є ключовою умовою успішного заповнення заяви на порталі Дія.

Олексій Вискуб також відвідав пологове відділення Центральної міської лікарні №1, де запуск «Малютко онлайн запланований на 1 листопада. Для цього у пологовому будинку запроваджується можливість реєструвати дитину в електронній системі eHealth.

«Зараз ми активно співпрацюємо з Міністерством охорони здоров'я та Національною службою здоров'я України над тим, щоб електронний медичний висновок був запроваджений у всіх пологових будинках України. До кінця року кожна українська сім'я, у якій народилася дитина, зможе отримати сучасний сервіс від держави без необхідності контактувати з нею. Швидко, зручно та навіть не виходячи з дому», – підкреслив Олексій Вискуб.

Запустити послугу «Малютко та об'єднати у ній 9 державних сервісів вдалося завдяки взаємодії реєстрів низки державних органів, яку налагодило Міністерство цифрової трансформації.

Після заповнення заяви на порталі Дія вона автоматично надсилається до Реєстру актів цивільного стану Мін'юсту. Там формується свідоцтво про народження дитини. Паралельно заява надсилається до державної податкової інспекції, де автоматично дитині присвоюється податковий номер. А також до Державної міграційної служби, де дитина реєструється в Єдиному державному демографічному реєстрі. І після автоматичних відповідей з цих реєстрів завершується формування свідоцтва про народження дитини у Мін'юсті. Цей документ в електронній формі надсилається до Міністерства соціальної політики, де відбувається призначення допомоги при народженні та інших видів соціальної допомоги, залежно від ситуації родини. Також заява та документи надсилаються до відповідного міста, де відбувається реєстрація місця проживання дитини (*Мінцифра пришвидшує запуск онлайн-послуги «Малютко в регіонах // <https://thedigital.gov.ua/news/mincifra-prishvidshuye-zapusk-onlajn-poslugi-yemalyatko-v-regionah>. – 2020. – 22.10).*

У Парламенті зареєстровано законопроект, який дозволить Мінцифрі запуснути проєкт Е-резидентство.

Це означає, що іноземці матимуть змогу вести бізнес в Україні за найпривабливішими умовами та без фізичної присутності на її території.

«Мінцифра формує цифрову економіку країни, залучаючи іноземців віддалено вести бізнес в Україні. Проєкт е-резидентство дозволить фрілансерам з ІТ та креативної сфери дистанційно вести бізнес в Україні та розвиватись через партнерство з авторитетними світовими компаніями. Це покращить національний імідж України на міжнародному ринку ІТ та наповнюватиме державний бюджет за рахунок податків», – наголошує **Віцепрем'єр-міністр – Міністр цифрової трансформації Михайло Федоров.**

Законопроект № 4240 «Про внесення змін до Податкового кодексу України та деяких інших законодавчих актів України щодо ведення підприємницької діяльності е-резидентами в Україні» ***дозволить врегулювати механізми оподаткування е-резидентів та створюватиме умови для:***

- дистанційної реєстрації е-резидентів як фізичної особи-підприємця;
- здійснення підприємницької діяльності в юрисдикції України;
- відкриття банківських рахунків онлайн;
- доступу до адміністративних послуг, використовуючи кваліфікований електронний підпис.

«Вже набула чинності Постанова «Про проведення експерименту із запровадження та реалізації в Україні електронного резидентства». Наступний крок – розробка відповідних нормативно-правових актів, якими затвердимо процеси надання послуг та сервісів для е-резидентів. Також вже підготовлено технічну документацію для функціонування інструментів е-резидентства та розробляємо вебпортал», – коментує **заступник Міністра цифрової трансформації з питань розвитку ІТ Олександр Борняков** (Мінцифра працює над впровадженням Е-резидентства в Україні // <https://thedigital.gov.ua/news/mintsifra-pratsyue-nad-vprovadzhennyam-e-rezidentstva-v-ukraini>. – 2020. – 22.10).

Міністерство цифрової трансформації пришвидшує цифровізацію сфери охорони здоров'я в умовах пандемії. Більше державних послуг стали доступними онлайн на порталі Дія.

«Мінцифри й надалі цифровізуватиме усі галузі економіки країни. Але медична сфера – наразі пріоритет для нас. Задля зменшення кількості нових випадків інфікування коронавірусом спільно із МОЗ активно працюємо над переведенням якомога більшого числа медичних послуг в онлайн», – наголосив **Віцепрем'єр-міністр – Міністр цифрової трансформації України Михайло Федоров.**

Для того, щоб усунути необхідність контакту з державними органами, Міністерство цифрової трансформації спільно з Міністерством охорони

здоров'я та Національною службою здоров'я України прискорили запуск по всій Україні комплексної послуги «Малютко онлайн». З 5 жовтня батьки новонародженої дитини можуть отримати до 9 державних сервісів за однією електронною заявою.

Зараз послуга «Малютко» доступна онлайн у 139 населених пунктах у 164 пологових будинках. Для цього Мінцифри усунуло головний бюрократичний бар'єр – паперовий медичний висновок про народження дитини. Тепер у лікарів є можливість у пологовому будинку зареєструвати дитину онлайн – зробити електронний медичний висновок. Батьки отримують у смс-повідомленні номер медичного висновку, за яким відбувається реєстрація народження дитини.

Запуск комплексної послуги «Малютко онлайн» став поштовхом до подальшої цифровізації медичної галузі. Згодом усі медичні довідки будуть замінені на електронний медичний висновок – відповідний запис у Реєстрі системи eHealth. Крім цього, зараз Мінцифри та МОЗ працюють над впровадженням електронних лікарняних, що стануть доступними впродовж двох місяців.

«Це ще одна революція у системі охорони здоров'я України – спрощення процедури отримання лікарняного та виплат, не лише полегшить життя українців, а й матиме суттєвий антикорупційний ефект. Економія для держави може сягнути до 5 млрд грн на рік», – зазначив Михайло Федоров (*Михайло Федоров: переведення медичних послуг в онлайн – пріоритет для Мінцифри під час пандемії // <https://thedigital.gov.ua/news/mikhaylo-fedorov-perevedennya-medichnikh-poslug-v-onlayn-prioritet-dlya-mintsifri-pid-chas-pandemii>. – 2020. – 21.10*).

Батьки 7 млн дітей віком до 14 років можуть сформувати цифрове свідоцтво про народження дитини у мобільному застосунку Дія 2.0.

Про це заявив **Віцепрем'єр-міністр – Міністр цифрової трансформації Михайло Федоров** у ефірі програми «Ранок з Україною».

«Ми запустили цифрове свідоцтво про народження у мобільному застосунку Дія. Це – можливість для обох батьків більше не переживати за наявність паперової копії документа. Адже воно має таку саму юридичну силу, як і його паперовий аналог. Для того, щоб його отримати, потрібно просто оновити застосунок Дія».

Цифрове свідоцтво про народження використовується для поїздок Україною, отримання банківських, медичних, освітніх послуг та інших.

Для того, щоб отримати цифрове свідоцтво про народження, перш за все потрібно встановити або оновити мобільний застосунок Дія. Далі обрати «Додати Свідоцтво про народження дитини» та ввести серію й номер документа. Так свідоцтво про народження з'явиться у смартфонах батьків.

Крім того, у мобільному застосунку Дія 2.0 доступна функція шерингу – можливість ділитися цифровими копіями документів. Так, батьки дитини

зможуть не носити із собою паперової версії свідоцтва про народження. А за необхідності шерити цифрову копію документа.

Важливо, що цифрове свідоцтво про народження в Дії має таку ж юридичну силу, як і його паперовий аналог. Якщо ж раптом цифрового свідоцтва не прийняли, необхідно відразу ж звернутися до служби підтримки Дії.

Юридичних підстав відмовити у використанні цифрового свідоцтва про народження дитини в Дії немає. Адже 23 вересня Кабінет Міністрів України затвердив постанову № 911, якою легалізував використання цифрового свідоцтва на рівні з паперовим. Також постановою визначено можливість передавання цифрового свідоцтва про народження у вигляді електронних копій (*Михайло Федоров: батьки 7 млн дітей можуть отримати цифрове свідоцтво про народження дитини у застосунку Дія // <https://thedigital.gov.ua/news/mikhaylo-fedorov-batki-7-mln-ditey-mozhut-otrimati-tsifrove-svidotstvo-pro-narodzhennya-ditini-u-zastosunku-diya>. – 2020. – 21.10).*

За оцінками експертів Global Market Insights, обсяг світового ринку цифрової охорони здоров'я в 2019 році у світі перевищив \$ 106 млрд. У середньому щороку планують приріст інвестицій у сферу цифрової охорони здоров'я на 28,5 %.

Сьогодні пропонуємо вашій увазі *топ 5 напрямків розвитку цифрової системи охорони здоров'я у найближчих 5 років:*

1. Мобільні додатки і фітнес-гаджети (mHealth)

Фітнес-гаджети знаходять відгук у споживачів завдяки популярності смартфонів, планшетів і в цілому мобільних платформ. За даними Statista, до кінця 2019 року обсяг світового ринку mHealth перевищив позначку в \$ 52,6 млрд.

2. Телемедицина

Оперативна діагностика, аналітика рідкісних захворювань, підбір препаратів, розробка і пошук молекул з використанням цифрових бібліотек – лише деякі з областей застосування телемедицини. У сукупності з інноваціями телемедицина ще й дозволяє проводити віддалений огляд пацієнта.

3. Віддалений моніторинг стану пацієнта

Інструменти віддаленого моніторингу включають в себе мобільні девайси, що аналізують стан пацієнта та дозволяють стежити за станом пацієнтів з хронічними захворюваннями за межами лікарняної палати.

4. Точкове лікування онкологічних захворювань

Інновації медицини пов'язані з напрацюваннями у сфері біотехнологій і охоплюють широкий спектр областей, від біофармацевтики, штучного запліднення і генного редагування до дизайну білків і розробки ліків.

5. Ресурси підвищення медичної грамотності для непрофесіоналів

Всесвітня організація охорони здоров'я зазначає пряму залежність між критичними показниками в охороні здоров'я (наприклад, високим рівнем смертності) і некомпетентністю населення в питаннях здоров'я. Саме тому медична грамотність – популярний напрямок розвитку у наступних 5 років (*Топ-5 напрямків розвитку eHealth на найближчих 5 років // <https://ehealth.gov.ua/2020/10/20/top-5-napryamkiv-rozvytku-ehealth-na-najblyzhchyh-5-rokiv>. – 2020. – 20.10).*

При Міністерстві цифрової трансформації України у співпраці та за підтримки ПРООН в Україні створюється Лабораторія інновацій.

Головна мета – впровадження інноваційних методів пошуку та впровадження рішень у державному секторі.

Ця лабораторія вперше запускається саме на базі Мінцифри, де буде випробовуватись організаційна модель лабораторії.

До Policy Lab ver 1.0 увійдуть три консультанти з питань інновацій. Робота первинної експертної групи з 3-х експертів *Policy Lab ver 1.0 включатиме* (але не обмежуватиметься):

- надання консультативної підтримки та робота з Big Data – даними опитувань або аналізом результатів фокус-груп та, потенційно, великими даними від бізнесу;

- тестування ідей і рішень, щоб з'ясувати, що працює, а що ні, коли йдеться про вирішення складних проблем;

- мобілізація партнерських відносин

Детальні вимоги до експертів і можливість заповнити заявку на вакансію експерта доступні на сайті.

Лабораторія інновацій спочатку працюватиме з листопада 2020 року до березня 2021 року. Накопичені уроки та досвід, оцінені наприкінці періоду, сприятимуть продовженню участі або перегляду методів співпраці (*При Мінцифрі створюється Лабораторія інновацій. Що це і навіщо? // <https://thedigital.gov.ua/news/pri-mintsifri-stvoryuetsya-laboratoriya-innovatsiy-shcho-tse-i-navishcho>. – 2020. – 13.10).*

9 жовтня 2020 року розпочався пілотний обмін електронними рахунками-фактурами за допомогою рішення eDelivery між обраними компаніями з України та Польщі.

Пілотний проєкт eDelivery, який впроваджується Програмою EU4Digital в рамках її діяльності на підтримку електронної торгівлі, є важливим кроком на шляху до забезпечення безпечного, надійного, доступного і ефективного обміну даними щодо транскордонних рахунків між країнами-партнерами СхП і ЄС. Рішення eDelivery, представлене Європейською Комісією, усуває основні недоліки поточного нестандартизованого обміну даними на паперових носіях, такі як додатковий фінансовий тягар, ланцюжок затримок та незахищені дані.

Компанії-учасники входять до числа найбільших гравців українського ринку:

Кернел – один з провідних і найбільших виробників соняшникової олії і основний постачальник сільгосппродукції.

Premier Food – національний лідер з надання комплексних послуг громадського харчування та поставок якісних м'ясних і молочних продуктів.

Розуміючи потенціал і значимість пілотного проєкту eDelivery, один з найбільших постачальників послуг електронного обміну даними (ЕОД) в Україні – EDIN – (також постачальник ЕОД для Premier Food) вирішив взяти участь і підтримати підготовчі заходи до пілотного проєкту.

Ми формуємо цифрову економіку країни. Для забезпечення безперешкодного обміну даними рахунків з польською стороною сертифікований постачальник послуг точки доступу до Peppol eDelivery – Edison S.A. – погодився брати участь в пілотному проєкті і підтримувати обмін даними з польського боку.

«Реалізація пілоту закладе фундамент для створення технічно-правових механізмів, за допомогою яких українські компанії зможуть надсилати та отримувати електронні документи від контрагентів з ЄС, США, Канади, Австралії, Сінгапуру та ін.», – підкреслив **проєктний менеджер пілоту eDelivery від Мінцифри Михайло Латинський**.

В Україні найперша точка доступу Peppol eDelivery була створена, обслуговується і управляється Державним підприємством «Дія» – підприємством, що належить до сфери управління Міністерства цифрової трансформації України.

Партнери, що беруть участь в транскордонній торгівлі, будуть обмінюватися даними рахунків в Мережі Peppol через eDelivery. Пілотний проєкт буде вважатися успішним, якщо компанії з України та Польщі зможуть обмінюватися стандартизованими даними рахунків-фактур у момент виставлення рахунку з використанням рішення eDelivery. При завершенні пілоту команда Програми EU4Digital підготує рекомендації щодо необхідних юридичних, організаційних і технічних коригувань, які необхідно внести для повномасштабного впровадження рішення на національному рівні.

Україна робить величезний крок до створення цифрової держави (***Мінцифра розпочала пілотний проєкт eDelivery // <https://thedigital.gov.ua/news/mintsifra-rozpochala-pilotniy-proekt-edelivery>*** – 2020. – 12.10).

Міністерство цифрової трансформації України та міжнародний технологічний холдинг ТЕСНІА підписали Меморандум про співпрацю щодо розбудови галузі інформаційних технологій, будівництва дата-центрів, розвиток кіберспорту та STEM-освіти. Серед підписантів Віцепрем'єр-міністр – Міністр цифрової трансформації України Михайло Федоров та керуючий партнер холдингу ТЕСНІА Юрій Лазебніков.

Співпраця передбачає реалізацію проекту Екотехнопарку в Херсонській області. В його основі – дата-центр потужністю до 500 МВт, який виконуватиме функції зберігання, обробки даних та 3D-рендерингу. Дата-центр планують побудувати із використанням новітніх технологій та із врахуванням турботи про навколишнє середовище. Тепло, яке виділятиме дата-центр, планують утилізувати в агрофермі, яка також буде частиною Екотехнопарку.

Для реалізації першої черги проекту планують залучити не менше \$200 млн інвестицій в інфраструктуру. Дата-центр буде обслуговувати обладнання вартістю близько \$1 млрд доларів. Об'єкт потребує не менше 200 робочих місць. Мінцифри підтримує проєкт та сприятиме його реалізації.

Віцепрем'єр-міністр – Міністр цифрової трансформації Михайло Федоров зазначає: «Україна – цифрова країна, в якій стрімко розвиваються ІТ-інновації. Ми поставили перед собою ціль подвоїти частку ІТ-сектору до 10 % ВВП України і така співпраця сприяє розвитку технологічної екосистеми та прискоренню цифрової трансформації країни. Будівництво такого потужного дата-центру дозволить Україні надавати послуги зі швидкісної обробки даних та створити нові робочі місця. Впевнений, що наша країна здатна стати найпотужнішим ІТ-хабом у Центральній та Східній Європі, який залучатиме міжнародні інвестиції в Україну та зміцнити наші позиції на світовій арені».

«Екотехнопарк – це нова ніша для масштабних інвестицій в українську ІТ-галузь. Для цього в нас є все: зручна для великих зарубіжних клієнтів географія між Європою та Азією, дешева електроенергія, швидкий та якісний інтернет. І найголовніше – таланти. Ми вдячні Міністерству цифрової трансформації за підтримку і бажання посилювати технологічну репутацію нашої країни», – говорить **керуючий партнер холдингу ТЕСНІА Юрій Лазебніков**.

«Реалізації цього проєкту сприятиме ухвалення законопроекту №3199 «Про внесення змін до Закону України «Про ринок електричної енергії», який дозволить системним інвесторам на прозорих умовах спеціального аукціону отримати конкурентний тариф і укласти довгостроковий договір на постачання електричної енергії з державними генерувальними компаніями. Адже побудова цього ЦОДу загальною потужністю до 500 МВт дозволить максимально завантажити всі шість енергоблоків Запорізької АЕС», – додав **заступник Міністра цифрової трансформації України з питань розвитку ІТ Олександр Борняков**.

Серед інших стратегічних напрямків співпраці міністерства та компанії – розбудова кіберспортивної інфраструктури, зокрема, будівництво кіберспортивних арен та готелів, розвиток STEM-освіти в Україні та реалізація проєктів корпоративної соціальної відповідальності.

Презентація меморандуму відбулася на новозбудованій арені кіберспортивного медіахолдингу WePlay Esports, який є частиною холдингу ТЕСНІА (*Дата-центр з інвестиціями в \$1 млрд: Мінцифри розпочинає*

снівпрацю з холдингом ТЕСНІА // <https://thedigital.gov.ua/news/data-tsentr-z-investitsiyami-v-1-mlrd-mintsifri-rozpochinae-spivpratsyu-z-kholdingom-techiia>. – 2020. – 07.10).

Президент Володимир Зеленський заявив про незворотність процесу діджиталізації. Він запевнив, що з 2021 року жодна держустанова не зможе вимагати від українців документи у паперовому вигляді.

Про це він сказав у ході саміту «Дія».

«2020 рік стане початком ери paper less. Це означає – ніяких більше паперів. Це стосується всіх державних органів. Жодна державна установа не зможе вимагати від українця жодних папірців чи довідок для надання тих чи інших державних послуг», – заявив Зеленський.

Він додав, що користувачів електронного додатку «Дія» уже 5 мільйонів, і процес діджиталізації – незворотній (*Ніяких більше паперів: Зеленський заявив про незворотність процесу діджиталізації // <https://www.rbc.ua/ukr/news/nikakih-bolshe-bumag-zelenskiy-zayavil-neobratimosti-1601894222.html>. – 2020. – 05.10).*

Національний банк спростив процедуру віддаленої ідентифікації та верифікації банківських клієнтів з цифровим паспортом у мобільному застосунку Дія.

Відтепер громадянам під час дистанційного відкриття рахунку в банку не потрібно фізично пред'являти ID-картку або біометричний закордонний паспорт, якщо вони мають цифровий паспорт або закордонний цифровий паспорт у мобільному застосунку Дія.

Скористатися цим методом зможуть усі українці, які мають біометричні документи – ID-картку та закордонний паспорт. Для цього їм потрібно встановити застосунок Дія на свій смартфон та верифікуватися для отримання е-паспорта або закордонного е-паспорта з допомогою BankID.

Цифровий паспорт – це цифровий аналог паперових документів у мобільному застосунку Дія. В електронному вигляді відображається інформація, яку містить ID-картка та біометричний закордонний паспорт громадянина України[1]. Цифровий паспорт більш надійний, ніж звичайний паперовий та не менш надійний, ніж його пластиковий аналог. Він дає можливість отримувати надійні дані про користувача з офіційних державних реєстрів.

Як будуть застосовувати новий метод ідентифікації та верифікації клієнта?

Використовувати цей метод банк зможе після підключення до систем Міністерства цифрової трансформації.

Загалом процес буде таким:

- банк запропонує потенційному клієнту ідентифікуватися в Дії через BankID;

- після вдалої ідентифікації у клієнта відобразяться цифрові документи, відповідно до даних, що містяться в державних реєстрах;
- через захищені канали банк отримає дані клієнта та додатково здійснить його фотофіксацію методом розпізнавання реальності особи;
- після цього клієнт зможе користуватися послугами банку.

Крім того, аналогічно клієнт зможе поділитися копією цифрового паспорта або закордонного цифрового паспорта і у відділенні банку.

Це зменшить час обслуговування клієнта, адже не потрібно буде робити копії паспорта, як це відбувається зараз.

Які переваги нового методу?

Фактично сьогодні це єдина можливість для фінансових установ дистанційно перевірити ідентифікаційні дані громадян, що містяться в державних реєстрах.

Перевагами цього методу є:

- простота використання;
- надійність для банків – такі ідентифікаційні дані отримані з надійного джерела;
- діджиталізація процесів та пришвидшення обслуговування клієнтів банків.

Коли банки зможуть запропонувати цей метод своїм клієнтам?

Міністерство цифрової трансформації України планує запуснути цей механізм після проведення тестування функціоналу. Водночас банкам знадобиться час для підключення до систем Міністерства цифрової трансформації та налаштування операційних процесів.

Детально цей механізм ідентифікації та верифікації висвітлений у постанові Правління Національного банку України від 02 жовтня 2020 року № 138 «Про затвердження Змін до Положення про здійснення банками фінансового моніторингу», що набирає чинності з 03 жовтня 2020 року **(Відтепер відкрити банківський рахунок можна дистанційно з цифровим паспортом // <https://thedigital.gov.ua/news/vidteper-vidkriti-bankivskij-rahunok-mozhna-distancijno-z-cifrovim-pasportom>. – 2020. – 02.10).**

Регіональні ініціативи

Тернопіль здобув нагороду у конкурсі «Дієва громада», що проводило Міністерство цифрової трансформації України. Про це повідомляє Тернопільська міська рада.

Як зазначив **Сергій Надал**, нещодавно було представлено демоверсію «Електронного кабінету тернополянина» і вже зовсім скоро він запрацює в повноцінному режимі. Також у місті працює такі електронні сервіси: електронні консультації та опитування, інтерактивні онлайн-карти, електронні запити, сервіс сіті-бот «Назар».

До слова, конкурс «Дієва громада» проводиться Міністерством Цифрової Трансформації України у співпраці із Програмою «Електронне урядування задля підзвітності влади та участі громади» (EGAP), що впроваджується Фондом Східна Європа та Фондом Innovabridge за підтримки Швейцарії (*Анастасія Флейтута Тернопіль отримав відзнаку у сфері цифрової трансформації // <https://www.tenews.org.ua/post/show/1603813404-ternopil-otrimav-vidznaku-u-sferi-cifrovoi-transformacii>. – 2020. – 27.10).*

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 Миколаївщини.

Згодом у рамках проєкту комп'ютери будуть передаватися бібліотекам у Закарпатській і Львівській областях.

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

Для чого це потрібно людям?

Заступник Міністра цифрової трансформації з питань євроінтеграції Валерія Іонан підкреслила, що забезпечення бібліотек технікою – це реальний крок до масштабного перетворення бібліотек по всій країні на сучасні хаби цифрової освіти, які стануть популярною і корисною локацією для місцевих мешканців. «Ми заручилися підтримкою партнерів для впровадження проєкту в національному масштабі. В тому числі завдяки цій ініціативі, мільйони українців безкоштовно навчатимуться цифрової грамотності», – наголосила Валерія Іонан.

У сучасному світі вже неможливо знаходитись в остронь від цифрових технологій. Перед українцями стоять нові виклики і вони мають опанувати нові знання, навіть якщо це важко та потребує зусиль. Бібліотеки є саме тим публічним простором, де людям буде зручно користуватись комп'ютерами безкоштовно, відмічає **генеральний директор директорату внутрішньої та гуманітарної політики Офісу Президента Вероніка Селега**. Таким чином

люди отримають можливість опанувати програму для навчання, роботи і розваг.

Для чого це потрібно бібліотекам?

Важливо, що проєкт «Дія.Цифрова освіта» дає змогу розвиватись не тільки громадянам, але й бібліотекам, які отримують комп'ютери.

Це новий рівень для роботи бібліотек, вважає виконувач функції **ГОЛОВИ** **Миколаївської ОДА Тетяна Стахевич.**

Зокрема, бібліотеки отримують змогу оцифрувати архівні фонди та завжди залишатися актуальними для читачів. «Можливість стати хабом для отримання цифрових знань – поштовх для розвитку бібліотеки», – каже Маріанна Ковеня, куратор проєктів фонду Favorit Foundation, який подарував комп'ютери.

Ще одна можливість для бібліотек – створення коворкінг-центру. Працюючи за комп'ютерами у затишних залах бібліотек відвідувачі зможуть зосередитись на навчанні чи роботі. З словами **Ганни Замазєвої – голови правління ВАФК, регіональний партнер Центру підтримки підприємців Дія.Бізнес у Миколаєві,** сучасна бібліотека так чи інакше все більше опирається на інформаційні технології – від допомоги у пошуку загальної чи наукової інформації до використання зовнішніх електронних баз даних.

Для чого це потрібно громадам?

Комп'ютеризація сільських бібліотек дає поштовх й розвитку громад, де вони розташовані. Президент ГО «ВГО Українська бібліотечна асоціація» Оксана Бруй наголошує, що цей проєкт є гарним прикладом взаємодії бізнесу, влади, громадянського суспільства і бібліотек. Оксана Бруй вважає, що комп'ютери, які сьогодні передано до бібліотек ОТГ та сільських бібліотек, стануть початком великих змін для кожної із цих бібліотек. Вони спонукатимуть і бібліотекарів, і місцеву владу розвивати свої бібліотеки і спроможності своїх громад.

Голова правління Асоціації розвитку туризму Фазиль Аскеров заявив, що передача комп'ютерів до сільських бібліотек – це підтримка вітчизняного бізнесу та державних програм у сфері цифровізації (*Мінцифри: бібліотеки Миколаївщини відтепер комп'ютеризовані // <https://thedigital.gov.ua/news/mintsifri-biblioteki-mikolaivshchini-vidteper-kompyuterizovani>. – 2020. – 21.10).*

Місто Львів здобуло перемогу у конкурсі «Дієва Громада» від Міністерства цифрової трансформації України у номінації «Кращий документообіг».

«Система електронного документообігу є основоположною інформаційною системою для реалізації управлінських процесів в органі місцевого самоврядування. З початку 2020 року у Львівській міській раді запрацювала оновлена система електронного документообігу на базі програмного забезпечення IT-Enterprise. Розвиток цієї системи реалізовується

за принципами ERP-системи (Enterprise Resource Planning System – Система планування ресурсів установи) – корпоративна інформаційна система.

На противагу попереднім системам електронного документообігу, що діяли в міській раді раніше та забезпечували лише реєстрацію документів, існуюча система є модульною та забезпечує реалізацію різних галузей управління, має потенціал до масштабування та взаємодії з іншими сервісами», – зазначають в управлінні ІТ ЛМР.

Зокрема, запровадження системи документообігу забезпечило не лише пришвидшення внутрішніх управлінських процесів, але надало розуміння шляхів підвищення ефективності діяльності структурних підрозділів. Саме тому сформовано план щодо запровадження розширення функціонування системи.

Також система електронного документообігу є одним з основних елементів впровадження сайту «Портал мешканця Львова» як єдиного порталу для взаємодії мешканців з міською радою.

За допомогою порталу мешканці матимуть можливість замовляти адміністративні послуги, надсилати звернення та запити в електронному вигляді, а також отримувати їх результати в режимі онлайн. Всі заявки, отримані з порталу, оброблятимуться працівниками структурних підрозділів мерії в єдиній системі документообігу. Це не потребуватиме від службовців роботи в різних системах, що в свою чергу спростить процес надання послуг для мешканців. Бета-версія порталу стане доступною для мешканців уже наприкінці жовтня 2020 року та надаватиме можливість отримання найпопулярніших адміністративних послуг, зокрема оформлення та видачі довідки про місце реєстрації громадянина (протягом року її замовляють 75 тис. разів).

Як відзначають в управлінні ІТ, у середньому протягом місяця в системі реєструють та обробляють 5700 заяв на адміністративні послуги, що надає міська рада, понад 4500 внутрішніх документів, 4000 звернень громадян, 3000 вихідних ініціативних документів, 1900 вхідних документів від юридичних осіб, 250 запитів на публічну інформацію.

Додамо, що система документообігу реалізовується ЛКП «Міський центр ІТ» та компанією ІТ Enterprise (*Львів переміг у категорії «Кращий документообіг» конкурсу «Дієва Громада» // <https://city-adm.lviv.ua/news/government/282201-lviv-peremih-u-katehorii-krashchyi-dokumentobih-konkursu-diieva-hromada>. – 2020. – 19.10).*

Мінцифри ініціює відкриття даних на місцях – у Харкові та Маріуполі сьогодні стали доступні перші аналітичні інструменти на основі відкритих даних по медичних закладах.

В умовах пандемії коронавірусу цифровізація, зокрема онлайн-сервіси для мешканців міст, дозволяють зменшити соціальні контакти та захистити своє здоров'я.

Маріупольська та Харківська міські ради за підтримки Міністерства цифрової трансформації та USAID/UK aid проекту «Прозорість та підзвітність у державному управлінні та послугах/TAPAS» запустили інтерактивну аналітику про роботу закладів охорони здоров'я на основі відкритих даних. На сайтах проектів міститься інформація про завантаженість лікарів, фінансування кожної з лікарень у місті, найпоширеніші захворювання, а також рекомендації щодо діагностики стану здоров'я та гарантованих державою послуг і вакцинації.

Переглянути візуалізації можна за посиланнями:

Медицина Маріуполя в цифрах – <https://texty.org.ua/d/2020/med-mariupol>,
Медицина Харкова в цифрах – <https://texty.org.ua/d/2020/med-kharkiv>.

Сервіси допоможуть вибрати сімейного лікаря, краще спланувати візит у лікарню, виходячи з пікових завантажень по днях, і дізнатися про найпоширеніші захворювання в місті та тенденції їх поширення. Також можна отримати рекомендації щодо діагностики стану здоров'я та гарантованих державою послуг і вакцинації в сімейного лікаря, терапевта або педіатра відповідно до статі та віку пацієнта.

Крім цього, для Маріуполя створений функціонал, що дозволяє аналізувати надходження та використання благодійної допомоги, а для Харкова – закупівлю медпродукції комунальними закладами. Уся інформація представлена в зручному форматі у вигляді аналітичних дашбордів.

Візуалізації розроблені на основі відкритих даних департаментів охорони здоров'я Маріупольської й Харківської міських рад, а також Національної служби здоров'я України та системи «Prozorro». Уся інформація є знеособленою і узагальненою, тобто не порушує медичну таємницю. Таким чином, ці набори даних можуть використовувати підприємці, дослідники, активісти й журналісти для створення власних продуктів та аналітики.

Відкриті дані сприяють більш прозорій роботі закладів охорони здоров'я. Користувачі можуть моніторити роботу сімейних лікарів щодо проведення прийомів та надання медичних послуг. Фінансування закладів коштом державного бюджету стає цілком підзвітним. Громадяни отримують інформацію про обсяг коштів, який надійшов у лікарню, та кількість послуг, що були надані. Аналіз даних про захворюваність дає змогу ухвалювати обґрунтовані управлінські рішення стосовно розвитку галузі охорони здоров'я (*За підтримки Мінцифри міста відкривають дані про лікарні // <https://thedigital.gov.ua/news/za-pidtrimki-mintsifri-mista-vidkrivayut-dani-pro-likarni>. – 2020. – 19.10).*

Департамент економіки і інвестицій Полтавської міськради підготував есе з описом кращих практик цифровізації міста Полтави та заповнив анкету, у якій зазначено інструменти цифровізації, що використовуються у інфраструктурі міста, муніципалітеті, комунальних закладах, при наданні адміністративних послуг.

Конкурс «Дієва Громада» є першим етапом оцінки цифрової трансформації міст та областей задля написання майбутньої стратегії цифрової трансформації регіонів. Сприяючи створенню інструментів цифровізації, Міністерство Цифрової Трансформації України створює можливості для рівного доступу громадян до електронних послуг, е-демократії, розвитку смарт сіті, підвищуючи ефективність роботи муніципалітетів та розвиваючи цифрові навички населення та посадових осіб органів місцевого самоврядування, зазначили у Полтавській міськраді.

Конкурс був організований Міністерством Цифрової Трансформації України у співпраці із Програмою «Електронне урядування задля підзвітності влади та участі громади» (EGAP), що впроваджується Фондом Східна Європа та Фондом Innovabridge за підтримки Швейцарії.

Це дало можливість громаді міста Полтави долучилось до регіональної спільноти з цифровізації та популяризації впровадження цифрових рішень в областях України, що дозволить у майбутньому залучати ресурси у громаду та здійснювати цифрову трансформацію.

Наразі бажання взяти участь у конкурсі надійшло від близько 700 громад. Більше 100 громад та міст пройшли опитування. Полтава була серед 63 громад та міст, які надали есе з описом своїх кращих практик цифровізації.

Команда цифровізації Полтавської міської ради була відзначена табличкою учасника конкурсу «Дієва Громада» (*Полтавська міська рада взяла участь у конкурсі «Дієва Громада» // <https://np.pl.ua/2020/10/poltavska-mis-ka-rada-vziala-uchast-u-konkursi-diieva-hromada>. – 2020. – 15.10*).

Експертний погляд

Ірина Брилянт, членкиня Асоціації правників України, керуюча партнерка АО «Дестра», адвокатка:

В умовах стрімкого розвитку інформаційних технологій і глобалізаційних процесів у світі актуальним є впровадження методів електронного урядування. Зокрема, електронне резидентство є одним із прогресивних методів сучасного урядування, який створює передумови для успішного ведення бізнесу із нерезидентами.

Водночас е-резидентство дасть змогу державі-резиденту контролювати легальність господарської діяльності й оподаткування таких суб'єктів.

25 червня 2020 року Кабмін постановою «Про реалізацію експериментального проєкту із запровадження та реалізації в Україні електронного резидентства» створив передумови для запровадження в Україні інституту електронного резидентства.

20 жовтня 2020 року був зареєстрований проєкт закону «Про внесення змін до Податкового кодексу України та деяких інших законодавчих актів України щодо ведення підприємницької діяльності е-резидентами в Україні».

Аналізуючи законопроект в цілому, варто зазначити, що він пропонує низку реальних новацій.

Вони здатні створити умови для отримання зацікавленими іноземцями та особами без громадянства, які набули статусу е-резидента, можливості реєстрації себе як фізичної особи-підприємця та ведення підприємницької діяльності без необхідності перебування в Україні.

Проте цей законопроект не містить заходів протидії кіберзагрозам і двостороннього захисту даних у разі е-резидентства відповідно до закону «Про основні засади забезпечення кібербезпеки України».

Утім, доцільно розглянути **ключові позиції законопроекту**.

Ним, зокрема, передбачається доповнення розділу XX Перехідних положень Податкового кодексу України підрозділом 10-1 «Ведення підприємницької діяльності електронними резидентами».

Цими змінами передбачаються тимчасові, до кінця 2022 року, особливості та правила ведення підприємницької діяльності електронними резидентами-підприємцями.

Водночас дія цього підрозділу не поширюється на електронних резидентів-фізосіб.

Позитивним є те, що в законопроекті пропонується встановити податковою адресою е-резидента, який зареєструвався як фізична особа-підприємець, місцеперебування адміністратора, за яким він береться на облік як платник податків, а не місцеперебування кожного окремого резидента задля запобігання махінацій зі зміни домену.

Водночас адміністратором виступає ДП «Дія», що здійснює заходи зі створення, адміністрування, технічної підтримки системи, а також забезпечує й відповідає за захист і безпеку інформації в системі.

Проте в законопроекті не йдеться про конкретні дані, програми та заходи безпеки, які б гарантували максимальний ступінь захисту інформації е-резидентів і держави.

Варто зауважити, що законопроектом чітко встановлено, що е-резидент здійснює державну реєстрацію себе як платника єдиного податку третьої групи спрощеної системи оподаткування, обліку та звітності.

Зазначається також, що е-резидент-підприємець не може використовувати працю найманих осіб.

Водночас законопроектом також запропоновано норму, згідно з якою е-резидент-підприємець може здійснювати виключно ті види господарської діяльності, які визначені Мін'юстом за погодженням із Мінфіном.

Передбачається подальше внесення змін до відповідних підзаконних актів, у яких будуть визначені види господарської діяльності, які здійснюватимуть е-резиденти, серед яких, зокрема, такі:

- видання комп'ютерних ігор (58.21 КВЕД);
- видання іншого програмного забезпечення (58.29 КВЕД);
- комп'ютерне програмування (62.01 КВЕД);
- інша діяльність у сфері інформаційних технологій і комп'ютерних систем (62.09 КВЕД);
- оброблення даних, розміщення інформації на вебвузлах і пов'язана з ними діяльність (63.11 КВЕД) тощо.

Вважаю, що встановлення цим законопроектом спеціальних правил звітування е-резидентів є інструментом ефективного контролю за своєчасністю та правильністю сплати ними податків.

Цілком співмірним заходом для цілей оподаткування є те, що е-резидент-підприємець зобов'язаний вести облік доходів, витрат і інших показників виключно в електронному вигляді та через електронний кабінет платника податків.

Щодо правильності обчислення е-резидентом-підприємцем сум податку, то вони можуть підтверджуватися виключно первинними та іншими документами, які складені в електронному вигляді та надіслані до перевіркового органу, засвідчені кваліфікованим електронним підписом, а також копіями таких документів, якщо вони були складені в паперовому вигляді.

Будь-які дані, що не підтверджені зазначеними документами, вважаються такими, що не існують, і не можуть враховуватися під час обчислення податкових зобов'язань е-резидента-підприємця.

Але є винятки – випадки, коли врахування таких даних призводить до збільшення розміру податкових зобов'язань чи збільшення обсягу інших зобов'язань такого суб'єкта.

Водночас будь-які суми коштів, що надійшли е-резиденту-підприємцю, визнаються його доходом і оподатковуються за ставкою, передбаченою пунктом 293.4 статті 293 Податкового кодексу, якщо підстави для надходження цих коштів не підтверджені документами.

Положення проєкту закону відображають і специфіку проведення Державною податковою службою України перевірок, що зумовлено специфікою підприємницької діяльності, яку проводить е-резидент-підприємець, й особливостями звітування.

Проєктом закону також зазначається, що е-резидент-підприємець подає податкову декларацію виключно в електронній формі через електронний кабінет платника податків.

Зазначеним проєктом закону також пропонується внести зміни до інших законодавчих актів України.

Зокрема, пропонується доповнити статтю 1087 Цивільного кодексу частиною четвертою й передбачити порядок проведення розрахунків фізичних осіб-підприємців, що зареєстровані електронними резидентами, виключно в безготівковій формі.

Документом також пропонується внести відповідні зміни до наступних законів України:

«Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування»;

«Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців і громадських формувань» тощо.

Отже, з огляду на зазначене вище, цей законопроект містить чіткі норми, які сприятимуть налагодженню умов для ведення бізнесу е-резидентами в Україні, створить механізм для залучення нових інвестицій, а також призведе до збільшення доходів державного бюджету завдяки наповненню його податками, що сплачуються е-резидентами.

Проте цей законопроект усе ж недостатньою мірою передбачає заходи з мінімізації виникнення кіберінцидентів і посиленого захисту інформаційно-цифрових даних нашої держави (*Законопроект про електронне резидентство: переваги та прогалини // <https://thepage.ua/ua/experts/zakonoprojekt-po-elektronne-rezidentstvo-pro-sho-mova>. – 2020. – 29.10).*)

Алексей Выскуб, первый заместитель министра цифровой трансформации:

Цифрова держава, яку ми будуємо, передбачає зміну формату відносин між людиною та державою. Саме людина та її комфорт зараз – у фокусі уваги.

Створюючи нові сервіси, ми в Мінцифрі концентруємося на ключових життєвих подіях. Народження малюка, очевидно, чи не найважливіша серед них. Саме тому ми багато уваги приділяємо сервісу «ЄМалятко», який від жовтня доступний ще й онлайн.

Він уже спрощує життя українців, дозволяє витратити час на дійсно важливі речі замість бюрократії та довгих черг для збору необхідних документів. **Про переваги та цифрові перемоги цього проєкту** – детальніше.

1. *Найбільш комплексна e-послуга у світі – перша електронна життєва подія*

Об'єднання декількох державних послуг в одну комплексну за життєвою чи бізнес-подією – це сучасний світовий тренд у сфері цифровізації. Адже доволі часто людина стикається з необхідністю отримати одразу кілька державних послуг для відкриття власної справи (наприклад, кав'ярні) чи оформлення певної життєвої події (скажімо, народження дитини).

Крім того, ці послуги надаються різними органами влади, але часто вимагають однотипних документів від заявника.

«Малютко онлайн»

Було:

- ✗ 37 документів
- ✗ 11 візитів до відповідних органів влади
- ✗ Купа втрачених нервів та часу

Стало:

- ✓ 1 сервіс
- ✓ 9 державних послуг
- ✓ До 20 хвилин на необхідні оформлення



«Малютко» є першою в Україні комплексною електронною послугою, яка дозволяє батькам новонародженої дитини за однією заявою отримати

одразу до 9 державних послуг, залежно від ситуації в родині. Серед них – такі базові послуги, як реєстрація народження дитини та допомога при народженні дитини. Раніше для їх отримання потрібно було здійснити 11 візитів та подати 37 документів. У середньому на це йшло 10 днів.

Подібний досвід реалізовано в Канаді та Сербії, де надається послуга при народженні «5 в 1», та в Австралії і Новій Зеландії – «3 в 1». Україна забезпечила «9 в 1». Фактично – послуга «єМалятко» є найбільш комплексною у світі, а Україна продовжує формувати світові тренди цифровізації державних послуг.

2. Перший електронний медичний висновок

5 жовтня 2020 року комплексна послуга «єМалятко» запрацювала повністю онлайн. Електронну заяву можна заповнити на порталі електронних послуг «Дія». Це стало можливим завдяки цифровізації першої медичної довідки.

Охорона здоров'я є сферою з найбільшою кількістю документації. Звісно, вся вона є паперовою, і навколо неї існує безліч зловживань та навіть корупції. Наприклад, в інтернеті будь-хто може легко придбати медичну довідку для відвідування басейну, отримання посвідчення водія або навіть листок про тимчасову непрацездатність (лікарняний). Останній завдає державі щороку збитків на сотні мільйонів. То що ж робити?

Усі ці довідки мають бути замінені на електронні медичні висновки – відповідний запис із електронним підписом лікаря в системі eHealth. І якщо будь-яка організація, наприклад, МВС, має законні підстави вимагати від громадянина підтвердження медичного стану, вона отримуватиме електронні дані з реєстру eHealth.

Справжність паперової довідки неможливо перевірити, а електронний медичний висновок з електронним підписом лікаря та електронною печаткою Національної служби здоров'я України – неможливо підробити. Крім зняття певного паперово-адміністративного навантаження та наведення ладу у сфері охорони здоров'я, електронні медичні висновки справлять мільярдний економічний ефект для країни.

Саме проєкт «єМалятко» став головним стимулом запровадження першого електронного медичного висновку – про народження, який прийшов на заміну медичному свідоцтву 103/о.

3. Демографічний реєстр країни

Демографічний реєстр є основою функціонування держави. На жаль, в Україні створення цього базового реєстру було розпочато лише у 2016 році. Сьогодні він містить вже понад 19 млн громадян України та наповнюється при видачі біометричних паспортів – закордонного або ID-картки.

Отже, дотепер вперше дитина потрапляла до реєстру та отримувала унікальний ідентифікатор УНЗР лише у віці 14 років або, в окремих випадках, при оформленні закордонного паспорту. Тобто ціле покоління дітей віком від 0 до 14 років поки що – поза реєстром, що значно звужує їхні можливості та ефективність держави.

Для вирішення цієї проблеми однією з послуг «єМалятко» передбачена можливість реєстрації дитини в демографічному реєстрі та отримання УНЗР одразу при народженні.

4. Податковий номер від народження

За відсутності єдиного унікального номеру громадянина саме податковий номер відіграє таку роль у житті українців. І так званий ПІН є й досі головним ключем для ідентифікації громадянина в реєстрах. Через еволюційний підхід наповнення демографічного реєстру роль ПІН ще не один рік буде визначальною.

На сьогодні зазвичай українці отримують цей номер у 14 років перед оформленням паспорта, адже ПІН є однією з підстав для видачі паспорта. І потребує двох візитів батьків із дитиною до органів податкової служби.

єМалятко
комплексний сервіс, з яким батьки немовлят отримують до 9 послуг за 1 заявою

Як отримати?

- Офлайн з допомогою адміністраторів
 - У пологових будинках (43), ЦНАП (83), ДРАЦС (97)
 - Де саме: bit.ly/eMalyatko
 - Для заяви потрібні: номер електронного медичного висновку або медичне свідоцтво про народження (довідка 103/0)
- Онлайн
 - На порталі Дія → diia.gov.ua/services/yemalyatko
 - Для заяви потрібні номер медичного висновку та КЕП (електронний підпис)

Доступні послуги

Категорія	№	Послуга
Базові	1	Держреєстрація народження – ви отримуєте свідоцтво про народження дитини
	2	Визначення походження дитини
Додаткові	3	Реєстрація в Державному реєстрі фізичних осіб-платників податків (присвоєння дитині номера платника податків)
	4	Внесення інформації про дитину до Єдиного державного демографічного реєстру з присвоєнням унікального номера запису (УНЗР)
	5	Визначення належності новонародженого до громадянства України
	6	Призначення допомоги при народженні дитини
	7	Реєстрація місця проживання новонародженої дитини
	8	Призначення допомоги на дітей, які виховуються в багатодітних сім'ях
	9	Внесення відомостей про дитину до Реєстру пацієнтів, що ведеться в центральній базі даних електронної системи охорони здоров'я

Дія Є

Комплексом послуг «єМалятко» передбачена можливість для батьків оформити ПІН дитині автоматично при народженні. Це надзвичайно зручно, особливо з урахуванням того факту, що все більше дітей починають раніше користуватися умовно дорослими послугами, наприклад, банківськими.

5. «Швейцарський годинник»

«єМалятко» – дійсно унікальний проєкт, який об'єднав державні послуги, що надаються Мін'юстом, Мінсоцполітики, Міністерством охорони здоров'я, Державною податковою службою (ДПС), Державною міграційною службою (ДМС), органами місцевого самоврядування тощо.

Якщо доволі спрощено, комплексна послуга працює таким чином:

- Електронна заява з порталу «Дія» засобами системи «Трембіта» надсилається до державного реєстру актів цивільного стану, де починається формування свідоцтва про народження.

- Паралельно заява передається до ДПС та ДМС, в яких автоматично формується ПН та УНЗ відповідно. Після відповідей від цих реєстрів завершується формування свідоцтва про народження.

- Надалі свідоцтво в електронній формі надсилається до відповідного територіального управління соціального захисту, де відбувається призначення допомоги при народженні та інших соціальних допомог.

- Також свідоцтво надсилається в електронній формі до відповідного органу місцевого самоврядування, де відбувається реєстрація місця проживання.

Це унікальний кейс для України, коли різні органи влади працюють так злагоджено та ефективно задля отримання єдиного результату – якісного сервісу для громадянина. Працюють, як деталі швейцарського годинника.

Зараз послуга «єМалятко» доступна онлайн у 139 населених пунктах у 15 областях. До кінця року Мінцифри запустить «єМалятко» онлайн по всій країні. Ця послуга стала стимулом для проведення цілої реформи всередині eHealth, і, як результат, з'явилася можливість молодим батькам отримати не паперовий, а електронний висновок про народження дитини. Цифрова трансформація України триває (*Проект «єМалятко»: 5 цифрових перемог // <https://www.pravda.com.ua/rus/columns/2020/10/21/7270666>. – 2020. – 21.10*).

Блоги та соціальні мережі

Олексій Гнатенко, адвокат. Старший партнер АО «Легал Хаус»:

Законопроект 4004 розширяє повноваження правоохоронних органів та ретроспективно зобов'язує операторів та провайдерів телекомунікацій надавати доступу до інформації про абонента.

Вересень цього року ознаменувався намаганням Верховної Ради України розв'язати проблему кіберзлочинності в Україні.

На розгляд депутатів був запропонований проект Закону № 4004 від 01.09.2020 про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів.

Проект Закону передбачає не лише внесення змін до Кримінального процесуального кодексу України, а й до Закону України «Про телекомунікації».

Основною ідеєю законодавців є закріплення порядку використання електронних доказів у кримінальному процесі. Така необхідність викликана поширеною практикою подання сторонами електронних доказів у кримінальних провадженнях та необхідністю застосування нового виду доказів у судочинстві.

Це своєю чергою обумовлено особливостями деяких видів злочинів, спосіб вчинення яких безпосередньо передбачає використання тих приладів та пристроїв, які оперують інформацією в електронному вигляді.

Ще однією підставою для таких змін є проблема сучасного кримінального судочинства, яка полягає у неможливості повноцінного використання інституту спеціальної конфіскації, оскільки на сьогодні так конфіскація не охоплює віртуальні активи та унеможлиблює їх примусове вилучення.

Сучасна організована злочинність активно використовує віртуальні ринки, діяльність яких не врегульована законом, а це своєю чергою створює умови для здійснення легалізації доходів, одержаних злочинним шляхом.

Відповідно до досліджень Міжнародного валютного фонду, в усьому світі не врегульовані законом віртуальні ринки надають можливість відмити гроші в розмірі від 2,17 до 3,61 трлн доларів США щорічно. Прикладом неконтрольованого віртуального ринку є Silk Road, обіг якого склав 1,2 млрд доларів США.

Але, повертаючись до змін, які пропонує проект Закону, чи зможуть вони розв'язати проблему кіберзлочинності та яким чином вони вплинуть на бізнес?

Що пропонує законодавець?

Проект Закону передбачає наступні зміни:

1. Кримінальний процес поповнюється новим видом доказів – електронні докази.
2. Впроваджується окремий порядок спеціальної конфіскації віртуальних активів.
3. Вдосконалюється процедура проведення негласних слідчих (розшукових) дій у кримінальних провадженнях щодо кіберзлочинів.
4. Вдосконалюється державно-приватна взаємодія правоохоронних органів та операторів телекомунікації під час проведення оперативно-розшукових заходів, негласних слідчих (розшукових) дій та тимчасового доступу до інформації, речей і документів.

Електронні докази

Як бачимо, новий проект Закону доповнює перелік процесуальних джерел доказів, включивши електронні докази до переліку доказів.

До електронних доказів буде відноситися інформація в електронній (цифровій) формі з відомостями, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження.

До таких доказів можуть належати:

- 1) електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо);
- 2) віртуальні активи;
- 3) веб-сайти, веб-сторінки;
- 4) текстові, мультимедійні та голосові повідомлення;
- 5) метадані;
- 6) бази даних;
- 7) інша інформація в електронній (цифровій) формі.

Як видно, законодавець вводить абсолютно нові поняття для кримінального процесу. І якщо поняття «віртуальні активи» відомо із Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового ураження», то значення слова «метадані» мало знайоме широкому загалу.

Якщо говорити простими словами, то метадані – це інформація про дані, яка дозволяє описати природу об'єкта.

У такому випадку важливо розуміти що саме буде вважатися метаданими, яким чином вони можуть отримуватися, за якими алгоритмами буде відбуватися їх опрацювання, зберігання та знищення?

А докази, які у проекті Закону згадуються як «інша інформація в електронній (цифровій) формі», взагалі створює підстави для вільного трактування що саме буде вважатися електронним доказом.

Нова редакція Закону не містить чітких відповідей на ці запитання, а інші нормативно-правові акти, які застосовуються у кримінальному процесі, не мають чітких визначень таких доказів.

Хоча проєкт Закону розмежовує поняття електронного документа як різновиду електронного доказу та інших документів, які подаються в електронній формі.

Спеціальна конфіскація віртуальних активів

Запропонований законодавцем порядок зберігання електронних доказів та розв'язання питання про спеціальну конфіскацію віртуальних активів процедурно не відрізняється від спеціальної конфіскації речових доказів і документів.

Такий підхід законодавця до спеціальної конфіскації не може сприйматися позитивно, оскільки регламентація процедур, що пов'язані з обігом та використанням віртуальних активів в Україні законодавчо не визначені.

Це пов'язано з одним із критеріїв віртуального активу – його здатністю до цивільного обігу, правове регулювання якого законодавчо не врегульовано.

Тому загальні підходи спеціальної конфіскації до віртуальних активів як до матеріальних об'єктів, не є ефективними та достатніми для вирішення завдань кримінального провадження без належного законодавчого врегулювання.

Зняття інформації з електронних інформаційних систем

Не може залишитися поза увагою норма, якою законодавець пропонує змінити процедуру проведення негласних слідчих (розшукових) дій в частині зняття інформації з електронних інформаційних систем.

Частину 2 статті 264 КПК України пропонується викласти у наступній редакції – пошук, виявлення і фіксація відомостей, що містяться в електронних інформаційних системах або їх частинах, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, є слідчою (розшуковою) дією, яка проводиться на підставі постанови прокурора, слідчого.

Суть не змінилася – якщо доступ до електронних інформаційних систем наданий власником або користувачем, такі відомості вважають законно отриманими.

Але нова редакція частини 2 статті 264 КПК України створює конфліктну ситуацію на майбутнє, оскільки зняття інформації з електронних інформаційних систем відбувається не на підставі постанови прокурора або слідчого, а на підставі ухвали слідчого судді.

Оскільки одним з різновидів втручання в приватне спілкування є зняття інформації з електронних інформаційних систем.

Це пряма норма, яка закріплена у частині 1 статті 258 та частині 1 статті 264 КПК України і забороняє втручання у приватне спілкування без ухвали слідчого судді.

У випадку прийняття цієї зміни слідчі будуть зможуть безпідставно втручатися у приватне спілкування громадян, посилаючись на норму частини 2 статті 264 та не звертаючи увагу на частину 1 статті 258 КПК України.

Таке положення речей є нічим іншим як розширенням прав слідчих та прокурорів, що призведе до порушення однієї із засад кримінального провадження – невтручання у приватне життя.

Особи, які мають право на тимчасовий доступ до інформації в електронній (цифровій) формі, речей і документів

Нові редакції статей 164 та 165 КПК України розширюють коло суб'єктів, яким надається тимчасовий доступ до інформації в електронній (цифровій) формі, речей і документів за ухвалою слідчого судді або суду.

Таке розширення здійснюється через зазначення лише найменування органу досудового розслідування або прокуратури, якому надається право тимчасового доступу до інформації.

Вважаю, що подібна невизначеність, яка пропонується законодавцем, не може сприяти дотриманню таємниці досудового розслідування та може призвести до зловживань стороною обвинувачення у кримінальному провадженні при виконанні ухвал про тимчасовий доступ до речей і документів.

Тимчасовий доступ до інформації, яка знаходиться в операторів та провайдерів телекомунікацій

Законотворці також пропонують суттєво розширити повноваження правоохоронних органів шляхом надання тимчасового доступу до інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо.

Такий підхід до доступу інформації, якою володіють оператори та провайдери телекомунікацій, не може бути застосований, оскільки він є ретроспективним.

Оптимальним було б зазначити що ця норма починає діяти лише з моменту набуття чинності змін до КПК України або з дати, яка зазначена у рішенні слідчого судді, який надає дозвіл на тимчасовий доступ до інформації.

Таким чином, даний законопроект містить суперечливі та ризиконебезпечні для громадян та бізнесу норми, які призведуть до погіршення їх стану у кримінальному провадженні (*Error 4004, або чим боротьба з кіберзлочинністю загрожує бізнесу та громадянам // <https://blog.liga.net/user/agnatenko/article/38280>. – 2020. – 30.10*).

Jaanika Merilo:

Готова ли Украина к электронным выборам?

Вчера читала у многих друзей и знакомых: «У нас же есть Дія, почему через нее не голосовали?»

Если коротко, Дія к этому еще не готова, но к следующим выборам, хотя бы пилотировать, надеюсь будет готова.

Long read не как советника Министра цифровой трансформации, а личное мнение, которое может совпадать или не совпадать с мнением Минцифры.

Единственные на сегодня в мире электронные выборы проводятся в Эстонии, где уже с 2005 года можно электронно голосовать за местное самоуправление, парламент или Европарламент, президента выбирают по другой системе.

На сегодня можно голосовать ID-картой, которая у 99 % населения, или MobileID. В прошлом году на выборах 47 % людей проголосовали электронно. Те, кому так удобней и кто хотел приходить на участки, хотя осталась и такая возможность.

Но к этому Эстония шла более 10 лет, создавая фундамент. У большинства жителей была ID-карта, провели масштабные обучения компьютерной грамотности, когда за 1,5 года обучили 100 000 пенсионеров, создали более тысячи пунктов доступа в интернет, потом открыли код программы голосования и на GitHub и т.д. И была полная уверенность в кибербезопасности, на сколько это возможно. Хотя каждый год и разные хакеры обещали взломать хотя бы один голос, чтобы дискредитировать систему, пока не получилось.

Что у нас сегодня в Украине?

- ID-карта есть у примерно 4,3 млн населения. Через нее в принципе можно дать цифровую подпись, но на участках нет возможности их считывать, нет программного обеспечения для выборов и защищенных каналов ид

- Для ID-карт нет программы для выборов и уверенности, что карту просто не передадут другому за ту же гречку или XX гривен;

- MobileID на сегодня, ну прямо, очень мало у кого. Нет уверенности, что уровень защиты на симке достаточно высокий, и что эту симку просто так не передадут.

- Есть Дія и она уже установлена у более 4 млн жителей. Выборы – это самое критично важное для существования государства, потому, и до запуска электронных выборов или даже пилота, должна быть 100 % уверенность в решении и безопасности до того, как запускать возможность голосовать. Например, создатели Дії утверждают, что Дія не сохраняет персональные данные, только передает запросы и ответы. Хорошо, но при выборах уже надо будет временно сохранять голоса? Как и где и безопасность еще данной несозданной системы.

Подытоживая, я верю, что на следующих президентских выборах можно будет проголосовать электронно, но это требует очень системной работы:

- над созданием полного решения системы выборов и полной уверенности в ее безопасности;

- в определении системы идентификации, в которой есть убежденность что вы – это точно вы и это вы и голосуете (БанкИД точно небезопасно, скорее идентификация через цифровую подпись);

- в определении стратегии голосования, т.е. можно ли кроме Дія голосовать и через ID-карту тем, у кого нет смартфонов;
- по разработке законодательства про электронные выборы с механизмами защиты от передачи голоса;
- еще много, много.

То есть, подытоживая, однозначно, сейчас не было готовности через Дію проводить выборы до решения данного перечня вопросов. Но я думаю, возможно, реально системно и много работая, до следующих выборов создать возможность пилота, и мы предлагали в том числе помощь и опыт эстонских специалистов.

И еще. Референдум во многом в техническом смысле требует всего того же, что и голосование, а вот опросы как раз, мне кажется можно проводить. Понимая, что выборка не будет репрезентативной, если хотеть коррелировать демографией (<https://www.facebook.com/jaanika.merilo>. – 2020. – 26.10).

Владислав Криклій – міністр інфраструктури України:

500 000

Скільки дозволів на міжнародні перевезення вантажів з моменту початку роботи транспортного порталу вже було замовлено станом на сьогодні. Сподіваємось, вам зручно користуватися та продовжуємо постійно працювати над поліпшенням і розширенням функціоналу.

Через єдиний транспортний портал електронних послуг <https://e-transport.gov.ua> можна у тому числі:

- ✓ замовити дозволи на міжнародні перевезення вантажів;
- ✓ отримати доступ до галузевої системи документообігу DocsET;
- ✓ отримати доступ до онлайн-трансляцій з пунктів видачі дозволів;
- ✓ в майбутньому подати заявку на польоти безпілотних літальних апаратів.

Зручного користування! (<https://www.facebook.com/vladkryklii>. – 2020. – 24.10).

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

Разговоры о четвертой промышленной революции и Индустрии 4.0 ведутся уже не первый год. Хайп это или реальность?

Термин «Индустрия 4.0» впервые появился в 2015 году, в статье основателя Всемирного экономического форума в Давосе Клауса Шваба. Основами «Индустрии 4.0» принято считать полную автоматизацию производственных процессов с использованием Big Data, робототехники, AI, машинного обучения, блокчейна, облачных сервисов и так далее. К сожалению, с *нынешним восприятием Индустрии 4.0 есть несколько проблем.*

Во-первых, очень часто шум вокруг Индустрии 4.0 раздувается искусственно. Многие технологии, которые представляют как нечто новое, появились уже давно. История IoT началась 80-х годах прошлого века. Использование облачных серверов начало набирать обороты в начале 1990-х годов. Первые AI проекты появились еще в 1960-х годах. Очень часто все эти громкие слова используют просто для продвижения товаров и услуг.

Во-вторых, три предыдущие индустриальные революции были спровоцированы резким развитием и внедрением новых технологий. Первую революцию спровоцировало появление паровых машин. Вторую – электричество. Третью – микропроцессоры. Без этих технологий переворот в промышленности и других сферах жизни был бы невозможен. Какая кардинально новая технология появилась сейчас? Резкого скачка в развитии не произошло.

Так стоит ли доверять всей этой шумихе вокруг Индустрии 4.0? Может быть то, что мы наблюдаем сегодня – не более чем очередной этап третьей цифровой революции, которая началась еще в 1950-х годах?

Вовсе нет. Четвертая индустриальная революция идет полным ходом. Она отличается от предыдущих лишь тем, что ее спровоцировало не одна технология, а множество.

Еще одна отличительная особенность Индустрии 4.0 – это ее темп. «В отличие от предыдущих, эта промышленная революция развивается не линейно, а скорее экспоненциально» – писал пять лет назад Клаус Шваб. И действительно, спрос на рынке меняется с постоянно растущей скоростью, объем данных, которые необходимо обрабатывать увеличивается, а времени на адаптацию к новым условиям у бизнеса становится все меньше.

Следует отметить и третий фактор, влияющий на ход новой индустриальной революции и отличающий ее от предыдущих трех. Это – роль государства. Никогда раньше власть не оказывала столь сильное влияние на бизнес, как сейчас. Законы, стандарты, регуляторы, инвестиционный климат, уровень коррупции, субсидии, налоговые льготы, торговые войны и так далее. С каждым годом влияние этих факторов становится все сильнее. Государство может стимулировать переход к Индустрии 4.0, а может и затормозить его.

Это прекрасно понимают во многих странах. Еще в 2011 году в Германии была принята программа Industrie 4.0 с бюджетом 200 млрд евро. Часть средств на нее выделяет государство, часть – инвесторы. В других странах подобные программы тоже существуют, причем в некоторых случаях государство обходится без привлечения средств частных компаний. Но дело даже не в бюджетных средствах, выделяемых государством на адаптацию промышленности к условиям Индустрии 4.0.

Всемирным экономическим форумом был опубликован доклад Readiness for the Future of Production Report, в котором оценивается готовность разных стран к новым экономическим реалиям. Любопытно посмотреть на данные по Украине. Судя по цифрам, Украина не готова к новой индустрии. Но не стоит

забывать о том, что паровые машины, которые стали двигателями первой индустриальной революции, начали массово внедряться на производстве не по королевскому указу. Это сделали предприниматели того времени по собственной инициативе, не опираясь на помощь свыше. Не стоит надеяться на государственную помощь. Ничто не мешает бизнесу самостоятельно осуществить четвертую индустриальную революцию. Было бы желание *(Индустрия 4.0 и государство // <https://blog.liga.net/user/avernyhora/article/38119>. – 2020. – 09.10).*

Дмитро Жуков, адвокат:

Особливості ведення справи в електронному суді.

08 жовтня в Україні святкується день юриста, тож вітаю всіх колег з професійним святом і бажаю, щоб невпинна діджиталізація лише допомагала у нашій діяльності.

Термін «Держава в смартфоні» вже давно став мемом в українському суспільстві, адже не проходить місяця, щоб не «висів» якийсь державний реєстр. Позавчора Президент презентував мобільний додаток «Дія 2.0», в ході якого зазначив, що це перший крок на шляху до побудови держави-сервісу. Може це й крок, однак, точно не перший, адже вже 2 роки функціонує підсистема «Електронний суд», яка була покликана прискорити та зменшити витрати на судові процеси.

Одразу спойлер – «не вийшло».

Електронний суд («ЕС») мав стати частиною Єдиної судової інформаційно-телекомунікаційної системи, яка була покликана перевести паперове судочинство в електронне, надати можливість миттєвого обміну документами між учасниками справи, сповіщати їх про засідання та проводити їх за допомогою відеоконференцзв'язку.

Блискучий стартап з типовою українською реалізацією: в одних судах ЕС працює майже на повну, в інших – частково, а треті – взагалі не реагують на подані в ньому документи. Склалася парадоксальна ситуація, коли в одному й тому ж столичному суді частина суддів нормально приймають документи через ЕС, а інші – залишають їх без руху, вимагаючи подати те саме у паперовому вигляді. Тож чи слід користуватися ЕС?

Знову спойлер – так!

В першу чергу, доступ до ЕС є корисним не тільки адвокатам, але й бізнесу (особливо, юрисконсультам), адже дозволяє з власного комп'ютера перевірити що відбувається з твоєю справою. По-друге, інформація про новий документ по справі з'являється протягом доби з моменту його подання, тож не потрібно навімання ходити до суду на ознайомлення, що в умовах карантину особливо складно і незручно.

Тож як це працює.

Насамперед, слід мати кваліфікований цифровий підпис та РНОКПП, адже на сьогодні справи підтягуються до особистого кабінету за ним. Навіть у разі подання позовної заяви у паперовій формі із зазначенням у ній свого

РНОКПП та відповідного клопотання, працівник апарату суду ще під час реєстрації справи надасть Вам до неї доступ в ЕС. У разі ж якщо справа розглядалася ще за позовом, поданим у паперовому вигляді без підключення до ЕС, в особистому кабінеті слід подати заяву про «підключення».

Візуально кабінет виглядає таким чином:

Електронний Суд
Офіційна електронна адреса

Повідомлення
Вибране
Мі справи
Заяви
Довірності
Статистика
Кошик

Мі справи
Список судових справ

ІНФОРМАЦІЯ ПРО СПРАВУ ★ ДОДАТИ ДО ВИБРАНОВОГО УПРАВЛІННЯ ДОВІРНОСТЯМИ 🔍 Пошук

	Номер справи	Суд	Мій процесуальний статус у справі	Дата реєстрації першого докумен...	Дата надходження останьог...
<input type="checkbox"/>	...	Господарський суд Київської області	Представник позивача	18.06.2020	29.09.2020
<input type="checkbox"/>	...	Солом'янський районний суд міста Києва	Представник позивача	08.09.2020	08.09.2020
<input type="checkbox"/>	...	Голосіївський районний суд міста Києва	Представник заявника	04.09.2020	04.09.2020
<input type="checkbox"/>	...	Винницький міський суд Вінницької області	Представник позивача	21.05.2020	18.08.2020
<input type="checkbox"/>	...	Окружний адміністративний суд міста Києва	Представник позивача	26.06.2019	14.08.2020
<input type="checkbox"/>	...	Господарський суд Київської області	Представник позивача	19.05.2020	05.08.2020
<input type="checkbox"/>	...	Сьомий апеляційний адміністративний суд	Представник позивача	23.06.2020	31.07.2020
<input type="checkbox"/>	...	Чернівецький окружний адміністративний суд	Представник позивача	24.07.2020	24.07.2020
<input type="checkbox"/>	...	Південно-західний апеляційний господарський суд	Представник відповідача	28.12.2018	22.07.2020
<input type="checkbox"/>	...	Господарський суд Закарпатської області	Представник позивача	28.12.2018	14.07.2020
<input type="checkbox"/>	...	Чернівецький окружний адміністративний суд	Представник позивача	30.06.2020	30.06.2020
<input type="checkbox"/>	...	Франківський районний суд м. Львова	Представник відповідача	28.12.2018	21.05.2020
<input type="checkbox"/>	...	Чернівецький окружний адміністративний суд	Представник позивача	12.05.2020	12.05.2020
<input type="checkbox"/>	...	Південно-західний апеляційний господарський суд	Представник позивача	29.08.2018	27.03.2020
<input type="checkbox"/>	...	Касаційний господарський суд	Представник позивача	31.05.2019	24.03.2020
<input type="checkbox"/>	...	Закарпатський апеляційний суд	Адвокат	30.03.2016	02.03.2020
<input type="checkbox"/>	...	Господарський суд Івано-Франківської області	Представник позивача	26.02.2019	30.12.2019
<input type="checkbox"/>	...	Касаційний господарський суд	Представник відповідача	31.12.2018	23.08.2019
<input type="checkbox"/>	...	Західний апеляційний господарський суд	Представник позивача	31.12.2018	27.03.2019

Всього: 19

Що цікаво, дата надходження останнього документа (крайній правий стовпчик) майже завжди не збігається з реальним станом речей, тож слід кожну справу перевіряти вручну.

Також з недоліків слід зазначити усічений функціонал вбудованого текстового редактора (неможливість додати таблицю, діаграму, smart-art, вирівняти текст за шириною тощо), невдалі оновлення (час від часу вимикається функція повідомлень на email про нові події у справі), відсутність доступу до документів інших учасників, якщо вони подані в паперовій формі тощо.

В цей же час, переваги у цілодобовості подання документів, оперативності отримання інформації про їх подання іншим учасником,

повідомлення про наявність судового рішення, а також хмарного сховища всіх матеріалів справи перекреслюють недоліки роботи ЕС. Таким чином його наявність є безперечно кроком уперед у розвитку судової системи, тож сподіваємося, що його функціонал буде суттєво покращений і незабаром будь-яка справа зможе пройти всі інстанції без друку жодного аркушу папера (*Електронний суд: гарний, поганий, злий // <https://blog.liga.net/user/dzhukov/article/38105>. – 2020. – 08.10*).

Тимофій Бадіков, голова правління у ГО «Платформа Здоров'я»:

05.10.2020, завершила роботу Робоча група з питань розробки проєкту Концепції електронної системи охорони здоров'я. Головний підсумок роботи – нам вдалося отримати компромісний документ, який враховує інтереси різних учасників процесу #eHealth. Це і пацієнтська та медична спільнота, і науковці, і бізнес, і міжнародні партнери України.

Відпочатку я був скептиком, не надто вірив, що процес дійсно буде робочим. Працюючи в робочій групі, я надав цілу низку своїх пропозицій, що стосуються захисту інтересів пацієнтів. Ці пропозиції роками збиралися та багаторазово подавалися на розгляд МОЗ та профільних робочих груп, але на них не звертали уваги. Цього разу мене та інших експертів нарешті почуто. В багатьох моментах мені вдалося переконати членів робочої групи. Зокрема, в проєкті Концепції враховані пропозиції, що стосуються доступу пацієнтів до своїх персональних даних та інших функціональних можливостей ЕСОЗ. Документ визнає, що є проблема недостатньо розвиненої національної медичної інфраструктури інформатизації та кадрової цифрової компетенції і ставить завдання це вирішити. Важливо, що Проєкт Концепції визначає роль місцевих органів виконавчої влади, органів місцевого самоврядування, закладів охорони здоров'я у забезпеченні розвитку е-здоров'я на регіональному та місцевому рівнях.

На жаль, є низка моментів, яку не було враховано в проєкті Концепції, однак є сподівання, що ці питання вдасться врегулювати суміжними документами.

Хочу подякувати Yaroslav Kucher, Марія Карчевич, експертам-членам робочої групи, які надали свої пропозиції. Робоча група дійсно стала робочою, учасники почали чути один одного та йшли на компроміс. Адже такі важливі багатосторонні процеси неможливі без компромісу.

В мене пішло немало часу для того, щоб Концепція розвитку ЕСОЗ, а згодом і Стратегія рухалися вперед. Та це дуже важлива робота. Сподіваюсь, що узгоджений робочою групою проєкт Концепції не буде надто змінений Урядом при проходженні всіх юридичних процедур. З моменту, коли цей документ буде прийнятий, нарешті можна буде сказати, що процес розбудови eHealth в Україні розпочався. До цього часу були та продовжуються експерименти.

Тепер завдання Робочої групи – напрацювати конкретний проєкт плану заходів з реалізації Концепції.

Перевага нашої робочої групи в тому, що вона збрала експертів з різним баченням, а Міністерство охорони здоров'я У країни зуміло забезпечити збалансованість документу. Це і є завданням міністерства, оскільки якщо враховуються інтереси лише однієї сторони, то йде великий спротив в просуванні всього процесу. МОЗ з цим завданням впоралося, що є великим плюсом (<https://www.facebook.com/badikov.t>. – 2020. – 06.10).

Зарубіжний досвід

Во время слушаний в Сенате США в среду глава Facebook Марк Цукерберг и руководитель Twitter Джек Дорси не смогли назвать ни одного конкретного пользователя – «носителя либеральной идеологии», публикации которого подвергались цензуре в этих социальных сетях.

Власти США предъявляют претензии Twitter и Facebook из-за цензуры, которой в социальных сетях по произволу администрации сервисов подвергаются консервативные СМИ и отдельные пользователи, включая президента. Компании обвинения в цензуре отрицают.

На последних слушаниях один из сенаторов-республиканцев попросил сначала Цукерберга, потом Дорси назвать хотя бы одного известного либерала или организацию, продвигающую либеральную идеологию, чьи посты были бы заблокированы или подвергнуты цензуре иным способом в Facebook и Twitter (в контексте политической ситуации в США и в связи с предметом слушаний в Сенате «либерал» означает «сторонник демократической партии», это определённо относится к самим Цукербергу и Дорси – ред.).

«Я могу предоставить целый список, но есть множество примеров, когда ваши коллеги-демократы возмущаются... когда при проверке фактов некоторые тексты отмечаются как недостоверные, а демократы не согласны с этим», – ответил Цукерберг.

«Я просил назвать лишь одно имя [носителя либеральных взглядов], человека или компании, в отношении которых вы применили цензуру», – продолжил настаивать сенатор. Он указал на то, что большинство участников слушаний легко назовут поименно известных консерваторов, публикации которых в Facebook и Twitter подверглись цензуре, и повторил свой вопрос, обращаясь к Дорси.

Ни Цукерберг, ни Дорси привести пример цензуры публикаций носителей либеральных взглядов не смогли.

Ранее в письме к Конгрессу Минюст заявил о намерении добиться того, чтобы онлайн-платформы «перестали подвергать цензуре правомерные высказывания и продвигать одни идеи в ущерб другим» (*Вика Рябова Руководители Facebook и Twitter на слушаниях в Сенате не смогли подтвердить примером непредвзятость цензуры в социальных сетях // <https://d-russia.ru/rukovoditeli-facebook-i-twitter-na-slushaniyah-v-senate-ne-smogli-podtverdit-nepredvzjatost-cenzury-v-socialnyh-setjah.html>. – 2020. – 29.10).*

Народный банк Китая опубликовал для общественного обсуждения, которое продлится месяц, законопроект о правовом статусе цифрового юаня.

Цифровой юань, насколько можно судить по машинному (translate.yandex.ru) переводу документа с китайского, представляет собой фиатные деньги в форме криптовалюты, эмиссию, оборот и способы использования которых контролирует Народный банк Китая.

Как следует из законопроекта, *цифровой юань – это полноценный юань в том смысле, что обычная (банкноты, монеты) и цифровая формы национальной валюты в финансовой системе государства существуют равноправно и одновременно.*

Все другие криптовалюты на китайском рынке для платежей в юанях запрещаются. Выпуск любых токенов, обеспеченных юанями, незаконен.

Законопроект лишь создаёт юридические основы для разработки технологических протоколов эмиссии и оборота цифрового юаня. Это не значит, что у Народного банка Китая нет технологий для цифрового юаня – эксперименты с ним идут в стране почти год.

Ещё раньше в КНР ввели ограничения на использование криптовалют, что, как теперь ясно, было частью плана введения цифрового юаня.

В сентябре 2017 года регулятор заявил о приостановке ICO в КНР, объяснив решение «серьёзной угрозой стабильности финансовой и экономической системы страны». В январе 2018 правительство Китая выпустило документ с призывом к региональным органам власти «активно ориентироваться» на закрытие операций по майнингу». В том же году Народный банк Китая распространил запрет оперировать криптовалютами на иностранные онлайн-площадки (*Центробанк Китая готов ввести в оборот цифровой юань – законопроект // <https://d-russia.ru/centrobank-kitaja-gotov-vesti-v-oborot-cifrovoj-juan-zakonoproekt.html>. – 2020. – 27.10).*

Правительство Германии одобрило законопроект, позволяющий спецслужбам «прослушивать» зашифрованные сообщения пользователей мессенджеров вроде WhatsApp – в целях борьбы с терроризмом.

Документ направлен в парламент.

В случае принятия парламентом закон разрешит спецслужбам мониторить не только текущую переписку, но и зашифрованные сообщения, отправленные ранее, с помощью «шпионского ПО».

Немецкие министры внутренних дел и юстиции заявили, что службы безопасности должны иметь в своём распоряжении технологии такого же уровня, как и преследуемые ими преступники. Доступ к зашифрованным переговорам злоумышленникам может предотвратить преступление, подчеркивают они.

Оппозиция выражает тревогу из-за того, что законопроект ослабляет защиту прав человека; некоторые журналисты опасаются, что после принятия документа их могут принудить раскрывать свои источники.

Правительство, однако, отмечает, что законопроект будет принят лишь после одобрения специальной парламентской комиссии по судебному надзору за перехватом коммуникаций спецслужбами.

В 2016 году WhatsApp ввёл тотальное сквозное шифрование (end-to-end), при котором никто кроме участников обмена сообщениями не может расшифровать данные – ни хакеры, ни правоохранительные органы, ни сотрудники WhatsApp. Вслед за WhatsApp сквозное шифрование ввело большинство мессенджеров.

В США требования открывать переписку по решению суда обсуждаются с 2015 года, когда Apple отказалась помочь ФБР с расшифровкой данных с телефона убийцы из Сан-Бернардино, утверждая, что расшифровать данные в iPhone невозможно. Позже Минюст США заявил, что справился с задачей самостоятельно. В июле 2020 в Конгресс США поступил законопроект «О правомерном доступе к зашифрованным данным».

В августе 2016 главы МВД Франции и Германии призвали Еврокомиссию разработать закон о доступе к зашифрованному контенту в мессенджерах.

В Великобритании IT-компании, использующие сквозное шифрование, обвиняют в пособничестве растлителям малолетних, наркоторговцам и террористам. Страны-участницы разведывательного объединения «Пять глаз» (в неё входят Великобритания, Канада, Новая Зеландия, Австралия и США) требуют внедрить бэкдор в шифрование таких приложений, как WhatsApp, Facebook, Instagram и других. Индия и Япония, также сотрудничающие с альянсом, поддерживают инициативу.

В декабре 2019 парламент Австралии принял закон, предписывающий технологическим компаниям предоставлять полиции доступ к зашифрованным данным пользователей IT-сервисов в случае, если эта информация нужна для борьбы с преступниками (*Вика Рябова В Германии одобрен законопроект о доступе спецслужб к зашифрованной переписке пользователей мессенджеров // <https://d-russia.ru/v-germanii-odobren-zakonoproekt-o-dostupe-specsluzhb-k-zashifrovannoj-perepiske-polzovatelej-messendzherov.html>. – 2020. – 23.10*).

Охорона здоров'я – один із найбільших секторів в латвійській економіці та становить 4,0 % ВВП.

Проте, наразі населення надає перевагу приватній медицині і 42 % громадян Латвії самостійно оплачують послуги в галузі охорони здоров'я. Саме тому уряд країни збільшив страхове покриття, що надається державою для просування приватних лікарських послуг.

Сьогодні завдяки електронному здоров'ю в Латвії пацієнти можуть легко отримати доступ до власних медичних записів за допомогою державного порталу електронних послуг (завірені усі медичні документи електронними підписами). Пацієнтам надаються послуги відповідно до медичних пакетів. Найпопулярнішими електронними пакетами медичних

послуг є: «Моя державна платна послуга охорони здоров'я»; «Мій лікар загальної практики»; «Дані моїх новонароджених дітей»; «Мої дані в реєстрі хворих на цукровий діабет».

Сучасна система електронного здоров'я Латвії складається з трьох основних рівнів:

Перший рівень – для бізнес-користувачів, які розробляють та створюють медичні системи;

Другий рівень – це державна система, що об'єднує усі ключові компоненти;

Третій рівень – це національна інфраструктура електронного врядування для обміну даними з реєстрами та відповідними структурами.

Концепцію електронної медицини розпочали розробляти в 2015 му році і з січня 2018 року перехід на систему eHealth став обов'язковим для всіх медичних працівників Латвії. Медики, які використовують систему eHealth, одразу відзначили її ключові переваги: вона дозволяє їм відстежувати історію хвороби пацієнта, включаючи минулі обстеження та тести, та допомагає уникнути дублювання.

Усі лікарні, майже всі аптеки та половина лікарів загальної практики в Латвії наразі уклали контракти на впровадження системи електронного здоров'я (*eHealth в свімі Латвія // <https://ehealth.gov.ua/2020/10/15/ehealth-v-sviti-latviya>. – 2020. – 15.10*).

Особенности использования Интернета гражданами Индии.

Индия является вторым по величине онлайн-рынком в мире с более чем 560 миллионами интернет-пользователей, уступая только Китаю. Уровень проникновения Интернета в Индии в 2019 году достиг 41 % от населения страны, что является существенным улучшением по сравнению с 31 % в 2018 году. На долю Индии приходится 21 % общего мирового роста интернет-аудитории, в 2019 году число пользователей Интернета в стране выросло почти на 100 миллионов человек – больше всех в мире (см. таблицу ниже).

По данным Statista к 2023 году в стране будет более 876 миллионов пользователей Интернета. В августе 2020 лишь половина из 1,37 миллиарда индийцев имеют доступ к Интернету.

Доступность Интернета в стране зависит от таких факторов, как пол и социально-экономическое положение. Так, в 2019 году в сельской местности в Индии насчитывалось 290 миллионов интернет-пользователей по сравнению с 337 миллионами городских интернет-пользователей. Большинство индийских пользователей Интернета – молодые люди в возрасте от 20 до 29 лет, эта доля чуть выше сельской местности. В стране гораздо больше пользователей-мужчин, чем женщин, это сильнее проявляется в сельских районах по сравнению с городскими.

№ п/п	Страна	Абсолютный прирост пользователей (чел.)	Относительный прирост пользователей (%)
1	Индия	97,885,011	21 %

2	Китай	50,666,155	6,7 %
3	США	25,379,895	8,8 %
4	Індонезія	17,300,000	13 %
5	Іран	16,241,877	29 %
6	Україна	15,325,054	60 %
7	Танзанія	14,560,898	173 %
8	Італія	11,490,731	27 %
9	Бангладеш	10,158,000	12 %
10	Бразилія	9,946,450	7,2 %
11	Філіппіни	9,000,000	13 %
12	Аргентина	6,801,754	20 %
13	Афганістан	5,694,586	142 %
14	Турція	5,027,251	9,3 %
15	Кот-д'Івуар	4,529,978	69 %
16	Камбоджа	4,500,000	56 %
17	Германія	4,322,056	5,8 %
18	Нігерія	3,572,903	3,8 %
19	Іспанія	3,541,726	9 %
20	Алжир	3,484,731	17 %

Прирост інтернет-пользователей по странам в 2019 году в сравнении 2018 годом».

Большая часть интернет-пользователей Индии выходит в Интернет через мобильные телефоны. В 2019 году около 400 миллионов человек (30 % процентов населения страны) составляли пользователи мобильного Интернета, ожидается, что к 2023 году этот показатель возрастет до 500 миллионов человек и составит 35 %.

Дешёвые тарифных планов на передачу данных наряду с различными правительственными инициативами в Индии направлены на то, чтобы сделать доступ к Интернету посредством мобильных устройств основным в стране.

К 2023 году в Индии предполагается почти 450 миллионов пользователей социальных сетей. Кроме того, ожидается, что доля населения Индии, имеющего доступ к социальным сетям, вырастет с 24 % в 2019 году до более 31 % в 2023 году. Самой популярной социальной сетью в стране является Facebook (280 миллионов пользователей), ни в одной другой стране такого числа пользователей Facebook нет.

Нормативное правовое регулирование информационных технологий

Основным законодательным актом Индии, регулирующим правоотношения в сфере информационных технологий, является закон об информационных технологиях 2000 г. (Information Technology Act, ИТА), в который внесены существенные изменения в 2008 году. Закон в основном касается электронных документов, цифровых подписей, определений

правонарушений в области информационной безопасности, а также отдельных аспектов защиты персональных данных и ответственности за преступления в цифровой среде.

ІТА содержит положения, которые защищают конфиденциальность данных в Интернете, однако при определенных условиях доступ к таким данным может быть предоставлен уполномоченным органам власти. ІТА предусматривает установление правительством национального стандарта шифрования, запрет анонимного использования Интернета, условия размещения контента в Интернете. Также ІТА устанавливает стандарты защиты данных компаний и наказания за размещение материалов, содержащих детскую порнографию, хакерскую деятельность и мошенничество. ІТА экстерриториален, он распространяет действие на преступления или правонарушения, совершенные вне Индии, если преступление касается компьютерных систем или компьютерных сетей, расположенных в Индии.

ІТА предусматривает использование цифровых подписей для аутентификации электронных записей и документов с использованием асимметричного шифрования. В Индии выпуск цифровых подписей является обязанностью контрольного удостоверяющего органа (ССА), который осуществляет выпуск цифровой подписи для конечных пользователей напрямую или через местные удостоверяющие центры: Национальный центр информатики, Институт развития и исследований в области банковских технологий и др.

ІТА устанавливает конкретные действия, считающиеся хакерскими: например, получение незаконного доступа к компьютеру, скачивание копий или информации, содержащейся в документах, повреждение компьютера вирусным программным обеспечением. За это грозит до трёх лет тюрьмы.

ІТА запрещает любые действия с цифровым контентом, изображающим детей в явно сексуальном виде. Такими действиями считаются публикация, передача, создание текста или изображений, сбор, поиск, просмотр, загрузка, реклама, продвижение, обмен детской порнографией. Запрещается соблазнение или побуждение детей к сексуальным действиям в Интернете. Термин «дети» определяется как любое лицо в возрасте до 18 лет, при том, что согласно законодательству Индии (как и России) возраст сексуального согласия составляет 16 лет. Санкция за нарушение закона – штраф 1 миллион рупий (примерно 1 миллион рублей) и/или лишение свободы на срок до пяти лет.

Нарушение конфиденциальности и неприкосновенности частной жизни также преследуется по закону. Наказание – штраф 100 тысяч рупий и/или лишение свободы на срок до трёх лет.

В Индии регулируется деятельность интернет-кафе (Cyber Cafe). Были случаи, когда интернет-кафе использовались для совершения различных киберпреступлений, например, неправомерного завладения паролем доступа к банковскому счёту, отправкой электронных писем с целью запугивания

получателей и др. В этой связи интернет-кафе считаются одним из ключевых посредников, деятельность которых необходимо было урегулировать.

ІТА предусмотрел определение «интернет-кафе» как любой организации, предоставляющей доступ к Интернету любому лицу, а также включил интернет-кафе в перечень интернет-посредников, распространив на них соответствующие требования.

Посредником согласно ІТА является как любое лицо, которое от имени другого лица получает, хранит или передает информацию или предоставляет какую-либо услугу в отношении данной информации. Посредниками считаются операторы связи, интернет-провайдеры, поисковые системы, сервисы онлайн-платежей, онлайн-аукционы, торговые онлайн-площадки и интернет-кафе.

Статья 79 ІТА предоставляет интернет-посредникам условный иммунитет от ответственности за действия третьих лиц. Например, посредник освобождается от ответственности в отношении любой сторонней информации, данных или ссылок на информацию или данные, предоставляемых или размещаемых третьими лицами. Обязательным условием в данном случае является отсутствие возможности контроля и мониторинга размещаемой и хранимой информации.

Посредник обязан удалять незаконный контент после получения сведений о его наличии на интернет-ресурсе. Таким образом, посредник обязан действовать только после получения распоряжения суда или уведомления от соответствующего органа государственной власти. Посредник не обязан самостоятельно проводить оценку контента.

В развитие положений ІТА в Индии приняты правила информационных технологий (Information technology rules). Это подзаконные акты, которые касаются четырёх сфер:

- правила, регулирующие методы и процедуры обеспечения безопасности и конфиденциальных персональных данных, которые требуют от организаций, хранящих конфиденциальную личную информацию пользователей, поддерживать определённые стандарты безопасности;
- правила для посредников, запрещающие контент определённого характера, устанавливают нормы, которым должны следовать посредники в отношении контента, проходящего через их системы, а также устанавливают ответственность некоторых категорий посредников за обеспечение соответствия содержания информации на сайтах указанным правилам.
- правила, касающиеся принципов деятельности для интернет-кафе, которые обязывают регистрировать интернет-кафе в уполномоченном органе власти, вести журнал учёта данных пользователей и историю использования ими Интернета;
- правила, касающиеся предоставления электронных услуг, которые позволяют правительству определять порядок предоставления определённых услуг, таких, как подача заявлений, выдача сертификатов и лицензий, в электронном виде.

Статья 69F ITA предусматривает такой состав преступления, как «кибертерроризм», под которым понимается намерение поставить под угрозу единство, целостность, безопасность или суверенитет нации посредством запрета доступа лицу, уполномоченному получать доступ к ресурсам компьютера, попытка проникнуть или получить доступ к ресурсу компьютера без разрешения, а также действия, связанные с установкой вредоносного программного обеспечения на компьютер, которые могут привести к смерти или травмам людей, повреждению или уничтожению имущества и др. Кибертерроризм наказывается пожизненным лишением свободы.

Закон ITA утверждает индийскую группу реагирования на компьютерные инциденты (CERT-India) как национальное агентство по вопросам киберпреступности и описывает её функции как организации, призванной обеспечить безопасность киберпространства. Состав и руководство группы назначается правительством Индии, среди обязанностей группы можно выделить следующие:

- Сбор и анализ информации о киберпреступности;
- Прогноз и оповещения о киберпреступлениях;
- Разработка и участие в исполнении чрезвычайных мер для обработки инцидентов кибербезопасности;
- Координация действий по реагированию на киберинциденты;
- Написание рекомендаций об устранении уязвимостей и технических документов, касающихся методов, процедур, способов предотвращения, реагирования и отчётности в области информационной безопасности.

Любой поставщик услуг, посредник, центр обработки данных, юридическое или физическое лицо обязаны предоставить группе CERT-India информацию по запросу. В случае непредставления информации поставщик услуг, юридическое или физическое лицо наказывается лишением свободы на срок до одного года или штрафом.

Правительственные структуры наделяются полномочиями издавать распоряжения о перехвате, мониторинге и дешифровке любой информации, формируемой, передаваемой, получаемой или хранимой на любых компьютерных ресурсах. Также устанавливаются правовые обязательства и гарантии, относящиеся к таким действиям государства.

ITA предоставляет право государственным учреждениям издавать распоряжения о блокировке открытого доступа к любой информации через компьютерные ресурсы, если такая блокировка необходима или целесообразна в интересах суверенитета, целостности, безопасности Индии и её международных отношений или в целях предупреждения побуждения к совершению соответствующих правонарушений, включая акты терроризма.

Специально назначенные государственные учреждения наделяются полномочиями контролировать, собирать и хранить данные или информацию, создаваемую, передаваемую либо получаемую с помощью любых компьютерных ресурсов.

Механизм блокирования открытого доступа к данным

Блокировка открытого доступа к любой информации через компьютерные ресурсы дополнительно регулируется правилами 2009 года, касающимися порядка и гарантий блокирования доступа общественности к информации.

Ключевые организации и должностные лица, принимающие участие в процедуре блокировки:

- организация: правительственные министерства и ведомства, как на центральном уровне, так и на уровне штатов, а также агентства центрального правительства;

- уполномоченный сотрудник: правительство назначает должностное лицо, в ранге не ниже ответственного секретаря, в качестве «уполномоченного сотрудника» с целью подготовки и направления распоряжения о блокировании доступа общественности к любой сгенерированной, переданной, полученной, хранящейся или размещенной информации на любом компьютерном ресурсе в соответствии с ИТА;

- главный сотрудник: каждая правительственная организация для целей реализации правил назначает одного из своих должностных лиц в качестве главного сотрудника, сообщая об этом центральному правительству и в департамент информационных технологий Министерства связи и информационных технологий Индии, а также публикует данные о нём на официальном сайте организации.

Комитет по рассмотрению запроса о блокировке состоит из уполномоченного сотрудника, который является председателем комитета, и представителей (рангом не ниже ответственного секретаря) из Министерства юстиции, Министерства внутренних дел, Министерство информации и телерадиовещания и Группы реагирования на компьютерные инциденты (CERT-India).

Заинтересованное лицо подает жалобу уполномоченному сотруднику одним из двух способов:

- через главного сотрудника правительственной организации, в этом случае жалоба отправляется ему, после проверки формальных оснований жалобы, главный сотрудник отправляет её уполномоченному сотруднику в установленном формате;

- через главного секретаря штата, в этом случае лицо отправляет свою жалобу секретарю штата, а в случае его отсутствия советнику главы штата для проверки, одобрения и последующего направления уполномоченному сотруднику.

Уполномоченный сотрудник обязан в течение 24 часов подтвердить получение жалобы, уведомив об этом отправителя жалобы.

Комитет рассматривает жалобу вместе с приложенной к ней информацией. Посредник или иное лицо, ответственное за размещение предлагаемой к блокировке информации, уведомляется уполномоченным сотрудником о поступлении жалобы. Для направления пояснений по жалобе

предоставляется 48 часов. Если посредник является иностранным лицом, он должен представить ответ на запрос в течение срока, указанного в запросе уполномоченным сотрудником.

Ответ посредника или иного ответственного за размещение информации лица на запрос может быть представлен как в письменной форме (для иностранных лиц только в письменной форме), так и лично. В данном ответе необходимо обосновать, почему контент не нарушает положения статьи 69А Закона ИТА.

Если посредник не является лично или не представляет письменный ответ, комитет рассматривает жалобу и даёт рекомендации уполномоченному сотруднику на основе имеющейся информации.

Рекомендации передаются через уполномоченного сотрудника секретарю департамента информационных технологий Министерства информационных технологий. Может быть рекомендована блокировка доступа.

Секретарь на основании рекомендаций комитета издает акт о блокировке доступа либо об отсутствии оснований для блокировки доступа соответствующей информации в Интернете. В последнем случае уполномоченный сотрудник информирует об отказе в блокировке главного сотрудника, а главный сотрудник – лицо, подавшее жалобу.

Вся процедура должна быть выполнена в течение семи дней с момента получения жалобы уполномоченным сотрудником.

В чрезвычайной ситуации секретарь может передать временное распоряжение, содержащее рекомендацию о блокировке, уполномоченному сотруднику, который изучает запрос и принимает решение в соответствии с ИТА. После рассмотрения запроса уполномоченным сотрудником и в случае его согласия на блокировку соответствующая информация направляется секретарю, который может затем принять временную меру (распоряжение) о блокировке доступа к информации. Однако комитет должен рассмотреть вопрос о правомерности принятия временной меры (распоряжения) в течение 48 часов после её принятия. На основании рекомендаций комитета секретарь примет окончательное распоряжение либо о блокировке, либо об отмене временного распоряжения.

Правила не определяют максимальный срок принятия окончательного распоряжения на основании рекомендаций комитета, что может повлечь злоупотребления со стороны органов государственной власти Индии.

В течение последних лет блокировке подвергались различные крупные ресурсы, причём иногда без каких-либо объяснений, как в случае с Tureraad и Blogspot в 2011 году. В том же году временно были заблокированы все файлохостинги, чтобы не допустить пиратского распространения фильма «Сингам». В 2012 году был заблокирован доступ к сервису Vimeo и нескольким торрент-сайтам. Также периодически блокировались сайты, аккаунты и группы в различных социальных сетях, связанные с политическими событиями и протестами против коррупции в стране. В 2013

году в Індії заблокували декілька десятків порносайтів, в 2014 году – 472 файлообменника і файл-хостинга (по просьбі Sony). В 2015-2016 гг. правительство Індії продовжило блокування порносайтів, а также достигло договоренности с Google, Microsoft и Yahoo о фильтрации в поисковых выдачах для индийского сегмента Интернета всей информации об абортах и определении пола детей во время беременности.

В сентябрі 2017 в Індії заблокували сайт соціальної мережі «ВКонтакте». Блокування стало тимчасовою заходом до отримання властями країни від адміністрації «ВКонтакте» гарантії видалення будь-яких посилань на гру «Синій кит», схильнувану підлітків до самоциду. На території Індії було зафіксовано як мінімум 10 випадків залучення підлітків в дану гру, які закінчилися самоубійствами (або спробами самоубійства). Внаслідок Індія розблокувала російську соціальну мережу після отримання запрошених гарантій.

Одним из последних и наиболее ярких примеров блокировки стало решение правительства Индии заблокировать 59 приложений из Китая. Серед цих додатків були сервіс для створення і перегляду коротких відео TikTok, для якого Індія є найбільшим зарубіжним ринком; додатки для створення спільнот і відеодзвінків від Xiaomi, найбільшого виробника смартфонів, продаваних в Індії; два додатки Alibaba Group (UC Browser і UC News); Club Factory, яка претендує на звання третьою за величиною в Індії компанією в електронній комерції, месенджер WeChat і інші.

Настільки масова блокування саме іноземних додатків є першим випадком в Індії, рівно як і в світі.

Приостановление предоставления телекоммуникационных услуг

В 2017 году правительство Индии приняло «Правила временного приостановления предоставления телекоммуникационных услуг в случае чрезвычайных ситуаций или угрозы общественной безопасности», предусматривающие возможность отключения сети Интернета в Индии либо преднамеренную дестабилизацию его работы со стороны государства. Данні правила представлялись властями Індії як тимчасові. Розробники в лиці компетентних державних органів не проводили публичних консультацій, які б дозволили б експертам дослідницьких організацій прокоментувати проєкт даних правил, хоча дана процедура передбачена і обов'язкова в відповідності з положеннями закону про телеграфію і парламентською процедурою підготовки нормативних правових актів в Індії.

Згідно з вказаними правилами рішення про припинення надання телекомунікаційних послуг може бути винесено посадовцем вищого рівня, відповідальним за внутрішню безпеку, як на рівні країни, так і на рівні штату. Поводом для відключення можуть бути «непреодолимые чрезвычайные обстоятельства». Рішення діє протягом 24 годин без дозволу Міністерства

внутренних дел Индии. При наличии такого разрешения максимальный срок действия распоряжения составляет пять дней, после чего распоряжение должно быть рассмотрено на предмет объективности и соответствия законодательству специальным комитетом, состоящим из высших должностных лиц законодательной, исполнительной и судебной власти, а также представителей штата. Приказы передаются операторам связи либо в письменной форме, либо по защищённым каналам.

Случаи ограничения доступа к Интернету

Правительство Индии объяснило законодательное закрепление ограничения доступа необходимостью защиты граждан от террористической угрозы и беспорядков. В 2017 году, после вступления в силу Правил, большая часть ограничений доступа пришлась на индийский штат Кашмир, который имеет спорный статус. Блокировки также совершались в Харьяне, Раджастхане, Уттар-Прадеше, Мадхья-Прадеше, Западной Бенгалии и Махараштре.

Однако одним из самых существенных и значимых для Индии ограничений доступа Интернету стало такое ограничение в Кашмире и Ладакхе.

Днем 4 августа 2019 в Кашмирской долине и некоторых районах Джамму и Ладакха перестали функционировать сети сотовой связи, интернет-услуги и стационарные телефоны. Никаких официальных распоряжений, на основании которых такие действия были предприняты, населению этих регионов представлено не было. Жители Кашмира оказались в информационной блокаде. Действия Правительства Индии сделали для журналистов невозможным поиск новостей, репортёрскую работу, публикацию и распространение интернет-изданий, а также распространение информации.

На основании статьи 32 Конституции Индии главный редактор Kashmir Times Анурадха Бхасин и лидер оппозиции в верхней палате индийского парламента, депутат от Джамму и Кашмира Гулам Наби Азад подали иски к правительству Индии в Верховный суд, с требованием обязать правительство Индии отменить любые приказы, уведомления, указания и распоряжения, которые предусматривают блокировку всех средств связи. Истцы подчеркнули, что ограничения привели к нарушению прав на свободу передвижения, свободу слова и выражения мнений, на свободную торговлю и свободу вероисповедания.

Представлявший позицию правительства Индии в суде Генеральный прокурор бывшего штата Джамму и Кашмир Тушар Мехта указал, что первоочередной обязанностью государства является обеспечение безопасности граждан и их имущества. По его мнению (официальная позиция правительства), у истцов – в отличие от государства – не было полной информации о происходящих событиях в Кашмире, а для объективной оценки действий властей необходимо рассматривать их в контексте не только современности, но и исторического прошлого региона.

Генеральный прокурор также указал, что государство стало жертвой как традиционного, так и «цифрового трансграничного терроризма», но даже в этих сложных условиях власти не нарушали право граждан на свободное перемещение.

Говоря об отключениях связи и Интернета, генеральный прокурор подчеркнул, что в Джамму и Ладакхе Интернет не отключали. Также он сообщил, что социальные сети, через которые можно отправлять сообщения и общаться с несколькими людьми одновременно, могут быть использованы в целях побуждения к насильственным действиям.

Целью властей при ограничении доступа к Интернету было недопущение рассылки сообщений из-за границы с целью осложнения обстановки на местах. Кроме того, посредством Интернета можно передавать ложные новости или изображения, а в даркнете существует возможность покупать оружие и запрещённые вещества.

Генеральный прокурор не представил суду оригинала официального распоряжения о приостановлении предоставления телекоммуникационных услуг по запросу суда.

В связи с этим суд постановил, что:

1) компетентные органы обязаны опубликовать все действующие распоряжения об отключении средств связи и Интернета и публиковать все распоряжения в будущем, чтобы пострадавшие могли опротестовать их в суде;

2) свобода слова и выражения мнений, а также право на работу, ведение торговли и предпринимательской деятельности с использованием Интернета пользуются конституционной защитой;

3) приостановление интернет-сервисов на неопределённый срок недопустимо;

4) любое распоряжение о приостановлении доступа к Интернету должно быть основано на принципе пропорциональности и не должно длиться сверх необходимого срока;

5) компетентные органы должны немедленно проверить все распоряжения, приостанавливающие работу интернет-сервисов, распоряжения, не соответствующие закону, должны быть отменены.

Через две недели после того, как суд вынес данное решение, 24 января 2020 года, в Джамму и Кашмир заработал мобильный Интернет, но только по технологии 2G. Доступ был открыт только к сайтам из одобренного властями Индии списка; доступ к социальным сетям в Кашмире по-прежнему отсутствует.

Затем 18 февраля отдел по борьбе с киберпреступностью полиции Кашмира начал расследование в отношении пользователей, обходящих запрет на использование социальных сетей при помощи VPN-сервисов. Несмотря на запрет VPN, заблокировать их работу у компетентных органов Индии не получилось. Основным ограничителем доступа Интернета в настоящее время остается низкая скорость передачи данных.

Проект правил регулювання соціальних мереж і платформ

В октябрі 2019 правительство Індії пропонує нові механізми регулювання контенту в Інтернеті. Для реалізації даних механізмів підготовлені зміни в правила інформаційних технологій, що стосуються правил для посередників. Основною метою вказаних змін є підвищення відповідальності посередників за публікуваний контент, а також забезпечення його прозорості.

С однієї сторони, технології привели до економічного зростання та соціального розвитку, з іншої – фіксується експоненціальний зростання ненавистнических висловлювань, фейкових новин, порушення громадського порядку, антинародної діяльності, клеветнических публікацій та інших незаконних дій з використанням інтернет-платформ та соціальних мереж. Тому розробка змін та посилення нагляду має допомогти усунути постійно зростаючі загрози, а також захистити територіальну цілісність, суверенітет та національну безпеку Індії.

Об'єкт правового регулювання в документі визначено дуже широко, визначення охоплює практично будь-яку онлайн-компанію – від соціальних мереж та платформ електронної комерції до інтернет-провайдерів.

Предлагаемый индийскими властями набор регулятивных мер можно разделить на четыре блока:

1) вимога до великих онлайн-платформ, таких як Facebook, Google, Twitter, відслідковувати протягом 24 годин за запитом правоохоронного органу походження контенту, який не відповідає місцевим законам (зокрема, порушує приватність, пропагує ненависть або вводять в заблудження), а також заблокувати користувача та видалити контент (впродовж 24 годин) з збереженням видаленого контенту протягом 180 днів в інтересах розслідування правоохоронними органами;

2) вимога для будь-якої платформи з більш ніж 5 мільйонами користувачів призначити контактну особу, яка буде доступною для зв'язу з представниками правоохоронних органів та їх представникам для координації спільних дій;

3) встановлення у провайдерів автоматичних технічних пристроїв для моніторингу трафіку, які дозволять ізолювати індійців від «протиправної інформації» шляхом видалення з соціальних мереж та платформ незаконного контенту;

4) вимога змінити стандарти шифрування повідомлень в месенджерах так, щоб влада могла відслідкувати відправителя.

Індійський досвід вкладається в світову тенденцію посилення інформаційної безпеки. В разі прийняття нового нормативного акту Індія приєднається до зростаючого списку країн, що регулюють

социальные сети – это Австралия, Китай и Сингапур и ЕС. До настоящего времени указанный нормативной акт не принят.

Политический скандал вокруг Facebook

Оппозиционная партия «Индийский национальный конгресс» (Indian National Congress) обвинило руководство индийского подразделения социальной сети Facebook в предвзятой политике информационной безопасности в отношении сообщений и постов членов правящей Индийской народной партии (Bharatiya Janata Party), ведущих к разжиганию межнациональной розни.

В августе 2020 Wall Street Journal выпустил статью о том, как политическая принадлежность пользователей влияет на реализацию политики информационной безопасности Facebook. В материале, в частности, фигурировали прямые цитаты сотрудников индийского подразделения Facebook, которые сообщали о получении инструкций непосредственно от директора по публичной политике индийского подразделения Facebook госпожи Анкхи Дас. Сотрудникам было предписано не применять санкции за нарушения правил общения в Facebook в случае, если нарушения совершались политиками из правящей партии Индии, поскольку иное могло навредить перспективам развития и интересам Facebook в Индии.

Ключевым обвинением в адрес индийского подразделения Facebook стало отсутствие санкций со стороны социальной в связи с заявлением Тайгера Раджи Сингха, члена правящей партии Индии, в отношении индийских мусульман.

Тайгер Раджа Сингх опубликовал пост в Facebook, где призывал к расстрелу мусульман-рохинджа, угрожал разрушить мечети и называл индийских мусульман «предателями». К марту 2020 года команда внутренней безопасности Facebook признала Сингха не только нарушителем правил общения в Facebook, но и опасным пользователем. В случае попадания в категорию «опасных пользователей» служба безопасности Facebook принимает во внимание не только посты, но и деятельность человека вне социальной сети и её возможные последствия.

Согласно выводам ответственных сотрудников-наблюдателей Facebook, риторика Раджи Сингха с учётом особенностей индийского общества может привести к вспышкам реального насилия. Таким образом, его аккаунт должен быть навсегда заблокирован на платформах компании по всему миру.

По информации WSJ, несмотря на настойчивые требования сотрудников-наблюдателей Facebook, ответственных за безопасность платформы, госпожа Анкхи Дас не позволила осуществить блокировку. Раджа Сингх продолжает активно действовать в социальных сетях, у него сотни тысяч подписчиков.

Более того, Анкхи Дас и Facebook получают претензии относительно обеспечения правящей партии Индии «режима наибольшего благоприятствования» в вопросах, связанных с выборами. В качестве

примера приводится случай, когда Facebook за несколько дней до начала выборов в нижнюю палату парламента Индии в апреле 2019 года провёл мероприятия по удалению недостоверной информации. К такой информации были отнесены публикации и посты, связанные с пакистанскими военными, а также с индийской оппозиционной партией «Индийский национальный конгресс».

Нормативное правовое регулирование персональных данных

ІТА предъявляет к компаниям требование разумных методов и процедур при обработке или передаче персональных данных и предусматривает ответственность за неспособность защитить такие данные. Однако определения понятия «персональные данные» нет, ІТА ограничивается лишь указанием на необходимость определения перечня таких данных правительством Индии на уровне подзаконного акта.

Такой подзаконный акт был принят в 2011 году в виде упомянутых ранее правил информационных технологий, устанавливающих методов и процедуры обеспечения безопасности конфиденциальных персональных данных или информации, содержащей такие данные (правила 2011 года).

Правила 2011 года относят к конфиденциальным персональным данным шесть типов данных и два типа информации, содержащей такие данные:

Конфиденциальные персональные данные	Информация, содержащая конфиденциальные персональные данные (информация ПД)
1. пароль; 2. финансовая информация, такая как банковский счёт, кредитная карта, дебетовая карта или другие платёжные данные; 3. состояние физического, физиологического и психического здоровья; 4. сексуальная ориентация; 5. медицинские записи и история болезни; 6. биометрическая информация.	1. любые детали, касающиеся конфиденциальных персональных данных и предоставленные юридическому лицу для предоставления услуги; 2. любая информация, полученная в соответствии с вышеуказанными пунктами корпоративным лицом для обработки, хранения или обработки в соответствии с договором или иным образом.

Таким образом, любой документ или другой фрагмент данных, который содержит хотя бы одну из шести категорий конфиденциальных персональных данных, которые предоставляются юридическому лицу для оказания каких-либо услуг или выполнения в соответствии с контрактом каких-либо действий, также будут конфиденциальными персональными данными.

Правила 2011 года распространяются на сбор, хранение и обработку персональных данных как в электронном виде, так и на бумаге, а также на те персональные данные, которые были собраны до принятия правил 2011 года.

Все юридические лица, которые собирают, получают, владеют, хранят или обрабатывают конфиденциальные персональные данные или информацию ПД, обязаны принять и реализовывать политику конфиденциальности. Такая политика конфиденциальности должна быть опубликована на веб-сайте юридического лица. Политика конфиденциальности должна ясно определять методы и процедуры организации в отношении сбора, получения, владения, хранения, передачи, обработки и защиты конфиденциальных персональных данных и информации ПД.

При сборе конфиденциальных персональных данных оператор таких данных должен получить предварительное согласие субъекта конфиденциальных персональных данных. Субъекту конфиденциальных персональных данных в соответствии с законом предоставляется возможность отзыва согласия на их обработку. В случае отзыва согласия лицо, владеющее конфиденциальными персональными данными, обязано удалить такие данные.

Поскольку согласие на сбор данных требуется только для конфиденциальных персональных данных, можно сделать вывод, что это положение не применяется к информации ПД

Правила 2011 года предусматривают, что для раскрытия конфиденциальных персональных данных любому третьему лицу требуется предварительное разрешение субъекта конфиденциальных персональных данных. Такое предварительное разрешение может содержаться в договоре между поставщиком конфиденциальных персональных данных и лицом, в соответствии с которым конфиденциальные персональные данные были предоставлены юридическому лицу.

Однако существует ряд исключений из правила относительно необходимости предварительного разрешения перед раскрытием каких-либо конфиденциальных персональных данных:

- если такие конфиденциальные персональные данные запрашиваются в письменной форме государственными органами с целью проверки личности или для предотвращения, обнаружения, расследования преступлений, а также судами в рамках судебного процесса;
- когда раскрытие информации требуется в соответствии с действующим законодательством.

Правила 2011 года не предусматривают никаких штрафов за их нарушение.

Однако ITA предусматривает для любого лица, включая посредника, которое раскрывает персональные данные без согласия субъекта таких данных, а также с намерением причинить этому лицу убытки, наказание в виде лишения свободы на срок до трёх лет и/или штраф до пяти тысяч рупий. ITA также предусматривает выплату компенсации за любую халатность со стороны юридического лица в поддержании разумных методов и процедур

безопасности, если такая халатность приводит к убыткам – но уголовное наказание не предусматривается.

В разработке находится законопроект, создаваемый по аналогии с европейским GDPR, он опубликован для обсуждения в июле 2018 г. В ноябре 2019 министр электроники и информационных технологий Индии представил обновлённый вариант проекта закона о защите конфиденциальных персональных данных, который предполагает:

- смягчить ограничения на локализацию и передачу данных;
- расширить сферу действия закона на анонимизированные данные;
- корректировку правовых оснований для обработки данных;
- новую политику конфиденциальности;
- смягчить уголовные наказания;
- расширить права личности;
- создать «песочницу» для поощрения исследований и разработки новых технологий в области кибербезопасности.

Государственные проекты, связанные с использованием персональных данных:

Система идентификации и аутентификации граждан Индии Aadhaar

Каждый гражданин может использовать систему Aadhaar для авторизации, в том числе с помощью биометрических данных (отпечатка пальца и/или скана радужной оболочки глаза). Кроме того, система предоставляет возможность электронной подписи eSign. Подписанные документы можно загрузить, передать, хранить в специальном облачном хранилище и платформе для выпуска документов и их сертификации DigiLocker. Персональные данные пользователей Aadhaar защищены от недобросовестного использования. Aadhaar также делает возможным использование унифицированного платёжного интерфейса.

Ещё недавно у большинства граждан Индии отсутствовало свидетельство о рождении, без которого невозможно было идентифицировать личность. Это приводило к тому, что государственные пособия не доходили до конечных получателей и оставались в руках посредников.

В 2008 году был запущен Aadhaar, во многом похожий на идентификацию граждан по номерам социального страхования в США. Однако Aadhaar должен был предоставить гражданам более широкие возможности. Правительство Индии заявляло, что программа будет добровольной и в первую очередь предназначенной для малообеспеченных граждан, которым нужно предоставить продукты питания базовые товары.

Спустя 10 лет Aadhaar, в которой хранятся фотографии, имена, адреса, отпечатки пальцев, снимки радужной оболочки глаза и уникальные 12-значные идентификационные номера граждан, стала крупнейшей в мире системой идентификации с биометрическими данными.

Из примерно 1,3 миллиарда граждан Индии идентификационную карту Aadhaar имеют 99 % взрослых.

Проект объединённого платёжного интерфейса UPI, который также разработан правительством в сотрудничестве с Aadhaar, многие жители страны, не имеющие счёта в банке, впервые для себя открыли для себя финансовые услуги. При помощи запущенного правительством приложения BHIM миллионы индийцев смогли расплачиваться электронными деньгами вне зависимости от того, в каком банке они имели счёта. Перевод средств в BHIM так же прост, как отправка текстового сообщения. Кроме того, оплачивать покупки можно с помощью сканирования QR-кодов. Приложение постепенно вытесняет из обихода граждан практически все операции с наличными.

На следующем этапе развития системы, который получил название Aadhaar Enabled Payments System, предполагается, что смартфоны станут ненужными. Люди смогут оплачивать покупки, проводя пальцем по специальному терминалу, который вместо пластиковых карт будет считывать отпечатки.

Правительство Индии предоставило возможность хранить водительские удостоверения в электронном виде в приложении DigiLocker, чтобы избавить людей от необходимости везде носить с собой бумажные документы.

Разрабатывается технология оформления для пожилых граждан медицинских карт, прикреплённых к номерам в Aadhaar. В них будет храниться информация о состоянии здоровья пациента, доступ к которой смогут получать доктора.

В базе данных Aadhaar неоднократно выявлялись фальшивые записи. Известно немало случаев, когда идентификационные номера в Aadhaar появлялись у животных. Карту Aadhaar однажды нашли даже у индуистского бога Ханумана. Причиной наличия фальшивых записей является то, что базу данных Aadhaar никогда не проверяли на устойчивость ко взлому, о возможности которого сообщали многие эксперты по безопасности, правозащитники, юристы и политики.

В Aadhaar не используются базовые принципы криптографии, и о безопасности проекта вообще известно очень немного. Представляется целесообразным открыть доступ к коду Aadhaar (что является обычной практикой в области ИБ), чтобы специалисты по безопасности могли бы проверить уровень безопасности, оценив риски и угрозы.

Специалисты и эксперты указывают на агрессивность проникновения Aadhaar в другие системы. Например, студенты большинства индийских штатов, желающие сдавать национальный тест для поступления на медицинские специальности, получили уведомление от образовательного совета о необходимости сообщить номер в системе Aadhaar. Наличие регистрации в системе Aadhaar стало обязательным условием для студентов, желающих сдавать экзамен для поступления на инженерные специальности в большинство технических университетов страны.

Верховный суд Индии вынес постановление с требованием к правительству Индии о необходимости привязки номеров мобильных телефонов всех абонентов в стране (около миллиарда) к их картам в Aadhaar. Новые абоненты смогут активировать контракт с мобильным оператором только через базу данных Aadhaar.

Подключение к системе Aadhaar, предоставление своих биометрических и иных персональных данных изначально было добровольным, однако впоследствии стало «добровольно-принудительным». Так, малообеспеченных людей подключали к системе Aadhaar и получали их данные, установив на уровне нормативных правовых актов положения о том, что государственные услуги и субсидии доступны только после регистрации и только при обращении в электронной форме.

Более того, наличие номера в Aadhaar является обязательным для получения зерна в соответствии с законом о национальной продовольственной безопасности. Регистрация в Aadhaar стала обязательной для оплаты газа по льготным расценкам.

Правозащитные организации Индии беспокоит вероятность того, что данные Aadhaar будут использованы для массовой слежки, этнических чисток и другой тайной деятельности.

В конце октября 2019 года правительство Индии объявило о планах запустить крупнейшую в мире систему распознавания лиц. Согласно проекту полиция 29 штатов страны и семи союзных территорий будет иметь доступ к единой централизованной базе данных, которая облегчит поиск преступников и пропавших без вести людей.

Масштабы предлагаемой системы описаны в документе, опубликованном Национальным бюро регистрации преступлений. Предполагается, что система распознавания лиц сможет сопоставлять изображения, полученные от растущей сети камер видеонаблюдения, с базой данных, в которую войдут фотографии преступников, фотографии из паспортов и изображения, собранные различными государственными системами, включая Aadhaar.

Система также позволит осуществлять поиск на основе газетных фотографий, изображений, отправленных гражданами, или фотороботов подозреваемых. Кроме того, система будет распознавать лица на записях из закрытых систем видеонаблюдения и оповещать полицию при выявлении людей из чёрного списка. Полицейских планируется оснастить портативными мобильными устройствами, которые позволят фотографировать лицо интересующего человека и мгновенно найти его в национальной базе данных с помощью специального приложения.

Предполагается, что новая система распознавания лиц может сыграть важную роль в поиске преступников, пропавших без вести лиц и при опознавании трупов. Кроме того, система поможет полицейским «выявлять преступные структуры».

Стратегия Индии в сфере кибербезопасности

Национальная политика в области кибербезопасности (КБ), утвержденная правительством Индии в июле 2013, является первым индийским доктринальным документом, который призван обеспечить комплексное и единое видение политических приоритетов индийского государства, частного сектора и общества в целом в отношении кибербезопасности.

Национальная политика КБ является важной промежуточной ступенью к разрабатываемой в настоящее время индийской национальной стратегии кибербезопасности.

Ключевая роль в обеспечении КБ для индийских пользователей, бизнеса и государственных органов в национальной политике закрепляется за частным сектором.

Основными целями национальной политики КБ являются:

- формирование высокого уровня доверия и уверенности в IT-системах;
- реализация мероприятий, направленных на обеспечение соответствия политики Индии в сфере информационной безопасности мировым стандартам;
- разработка нормативной базы для обеспечения безопасности киберпространственной экосистемы;
- развитие механизмов получения информации об угрозах для IT-инфраструктуры, создание сценариев реагирования на национальном и отраслевом уровнях;
- усиление защиты и устойчивости критически важных компонентов национальной информационной инфраструктуры через обеспечение эффективного функционирования национального центра защиты критически важной информационной инфраструктуры (НСИРС) и распределения прав на проектирование, приобретение, разработку, использование и эксплуатацию информационных ресурсов;
- разработка передовых технологий в сфере безопасности, способствующие широкому распространению безопасных IT-продуктов для удовлетворения требований национальной безопасности;
- создание инфраструктуры для тестирования и проверки безопасности IT-продуктов;
- проведение мероприятий по подготовке кадров в области кибербезопасности;
- предоставление налоговых льгот предприятиям для принятия стандартов безопасности;
- обеспечение защиты информации во время ее обработки, хранения и передачи в целях защиты конфиденциальных персональных данных и уменьшения экономических потерь из-за киберпреступности;
- обеспечение эффективного предотвращения, расследования и судебного преследования киберпреступности, расширения возможностей

правоохранительных органов, в том числе посредством актуализации соответствующего законодательства;

- создание культуры кибербезопасности и конфиденциальности;
- укрепление глобального сотрудничества в сфере кибербезопасности.

Для создания механизмов раннего предупреждения угроз, управления уязвимостями и ответа на угрозы функционирует группа экстренного реагирования на компьютерные инциденты (CERT-India). С целью защиты национальной инфраструктуры создан NSIIRC.

Миссией NSIIRC является принятие необходимых мер для содействия защите критической информационной инфраструктуры от несанкционированного доступа, воздействия, использования, обнародования, разрушения, нарушения функциональности, взаимодействия и повышения информационной безопасности всех заинтересованных сторон.

Функции NSIIRC:

- осуществление деятельности в качестве государственной головной организации, ответственной за все меры по защите критической информационной инфраструктуры страны;
- разработка рекомендаций, направленных на снижение уязвимости критической информационной инфраструктуры;
- выявление всех критических элементов информационной инфраструктуры;
- стратегическое обеспечение деятельности правительства Индии по реагированию на киберугрозы безопасности в отношении критической информационной инфраструктуры;
- координация, обмен данными, мониторинг, сбор, анализ и прогноз угроз для критической информационной инфраструктуре для раннего предупреждения и оповещения (на национальном уровне);
- помощь в разработке планов, разработка стандартов, обмен передовым опытом и совершенствование закупок, связанных с защитой критической информационной инфраструктуры;
- разработка стратегии защиты, политик, оценок уязвимостей, аудита, методологий и планов по их распространению и внедрению для защиты критической информационной инфраструктуры;
- проведение научных исследований и развития смежных видов деятельности для защиты критической информационной инфраструктуры;
- разработка и организация программ обучения и информирования, развитие аудита и органов по сертификации для защиты критической информационной инфраструктуры;
- разработка и реализация национальных и международных стратегий сотрудничества в целях защиты критической информационной инфраструктуры;
- разработка рекомендаций в области защиты критической информационной инфраструктуры, предупреждения и ликвидации

последствий по согласованию с заинтересованными сторонами и тесной координацией CERT-India).

В июне 2018 года правительство штата Телангана на юге Индии в партнерстве с советом безопасности данных Индии (DSCI) создало центр передового опыта по кибербезопасности (CoE), внимание которого сосредоточено на стратегических областях, включая инновации, предпринимательство и наращивание кадрового потенциала.

Направления работы CoE:

- создание инновационной экосистемы на государственном уровне,
- сотрудничество с существующими инкубаторами и акселераторами развития,
- наращивание технологического потенциала.

Стратегия кибербезопасности была представлена на 12-ом саммите по безопасности Индии «На пути к новой национальной стратегии кибербезопасности» в августе 2019. Стратегия в настоящее время опубликована для обсуждения профессиональным сообществом. Самым важным требованием к интернет-безопасности, обозначенным в стратегии, является развитие эффективной координации между министерствами, а также обеспечение защиты критической национальной инфраструктуры и вовлеченность в реализацию мероприятий в сфере информационной безопасности в равной степени как государственного, так и частного сектора.

В стране с 2006 года действует программа «**Цифровая Индия**».

Принципы и методология программы:

- управление ИТ-инфраструктурой осуществляется государством, которое также способствует развитию стандартов и руководящих принципов, оказывает техническую поддержку, наращивает потенциал в этой области, проводит научно-исследовательские и опытно-конструкторские работы;
- увеличение объемов, переработка, использование интегрированных и совместимых систем, а также развёртывание новых технологий, таких, как облачные хранилища, будут проводиться в целях улучшения качества предоставления государственных услуг гражданам;
- регионам будет предоставлена возможность введения проектов, специфичных для каждого региона в отдельности, в зависимости от их социально-экономических потребностей;
- поддержка частных предпринимателей в выполнении проектов цифрового управления;
- минимум в 10 министерствах должна быть создана должность ИТ-директора для более быстрой реализации различных проектов электронного управления.

Структура управления программой включает в себя управляющий комитет, возглавляемый премьер-министром, консультативную группу, правительственный комитет по экономическим вопросам, комитет по контролю выполнения программы, комитет по незапланированным расходам, совет руководителей реализации целей проекта.

Программа «Цифровая Индия» предусматривает создание инфраструктуры электронного правительства. Индийские власти используют программное обеспечение с открытым исходным кодом для построения электронного правительства. Бесплатное и открытое ПО должно считаться приоритетным для всех новых проектов электронного государственного управления, реализуемых федеральными ведомствами и властями штатов Индии. IT-системы, которые работают на базе проприетарного ПО, должны будут перейти на open source.

Федеральным и государственным органам предписаны преференции для открытого программного обеспечения при государственных закупках. В случае желаяния или необходимости использования проприетарных продуктов государственные заказчики обязаны объяснить причины выбора таких решений.

Однако не все сервисы государственных услуг гражданам и бизнесу будут построены на открытых продуктах. Предусмотрены исключения в тех областях, где с функциональной точки зрения невозможно использование софта с открытым исходным кодом или нет достаточного опыта для внедрения таких решений. Кроме того, преференции для open source могут быть сняты в случаях, когда речь идёт о срочных и стратегически важных проектах. Для указанных целей может быть использовано проприетарное ПО, созданное индийскими разработчиками...

Выводы

В Индии существует система нормативных правовых актов, регулирующая различные сферы, в том числе информационных технологий, незаконного контента, социальных сетей и мессенджеров, персональных данных, электронной подписи, интернет-кафе и т.д.

Приняты или в ближайшее время будут приняты стратегические документы по кибербезопасности и защите от киберугроз. Вместе с тем существуют не урегулированные или не в полной мере урегулированные вопросы, среди них защита интеллектуальных прав на контент в Интернете, основания и условия ограничения доступа к Интернету для граждан, безопасность биометрических персональных данных.

В Индии также существует опыт массовых ограничений доступа к Интернету.

Следует обратить внимание на предложенные в октябре 2019 года Правительством Индии новые механизмы регулирования контента в Интернете. Для реализации данных механизмов подготовлены изменения в правила информационных технологий, касающиеся правил для посредников. Основной целью указанных изменений является повышение ответственности посредников за размещаемый контент, а также обеспечение его прозрачности.

Предлагаемый индийскими властями набор регулятивных мер можно разделить на четыре блока:

1) требование к крупным онлайн-платформам, таким как Facebook, Google, Twitter, отслеживать в течение 24 часов по запросу правоохранительного органа происхождение контента, который не соответствует местным законам, а также блокировать пользователя и удалять контент (в течение 24 часов) с сохранением удалённого контента в течение 180 дней для возможного расследования правоохранительными органами;

2) требование для любой платформы с более чем 5 миллионами пользователей назначить контактное лицо, которое круглосуточно и ежедневно будет доступно для связи с представителями правоохранительных органов и их представителям для координации совместных действий;

3) установка у провайдеров автоматических технических устройств для мониторинга трафика, которые позволят изолировать индийцев от противоправной информации путём удаления из социальных сетей незаконного контента;

4) требование к стандартам шифрования сообщений в мессенджерах с тем чтобы власти могли отследить отправителя.

Представляется интересным опыт Индии в рамках государственного проектов, связанных с использованием персональных данных (*Александр Федотов Опыт регулирования информационного пространства в Индии // <https://d-russia.ru/opyt-regulirovanija-informacionnogo-prostranstva-v-indii.html>. – 2020. – 14.10*).

Парламентское расследование в Британии выявило «явное свидетельство сговора между Huawei и китайским государством», и теперь комитет по обороне требует, чтобы вся продукция Huawei была удалена из сетей к 2025 году.

В июле британское правительство официально обязало британских операторов мобильной связи удалить всё оборудование Huawei из сетей 5G в течение семи лет, к 2027 году, напоминает издание. Британским операторам запрещено покупать оборудование Huawei с конца этого года.

Комитет по обороне Палаты общин в 91-страничном отчёте, посвящённом безопасности 5G, заявил о необходимости ускорить удаление оборудования Huawei из британских сетей, а также стимулировать развитие промышленных мощностей в Великобритании и привлечение других поставщиков.

Депутаты хотят, чтобы правительство поддержало предложение о создании альянса, состоящего из десяти крупнейших «демократических стран мира», чтобы создать альтернативу китайским технологиям и для борьбы с «технологическим господством авторитарных государств» (*Британский парламент заявил о «явных связях» Huawei с китайским правительством // <https://d-russia.ru/britanskij-parlament-zajavil-o-javnyh-svjazjah-huawei-s-kitajskim-pravitelstvom.html>. – 2020. – 08.10*).

Іванка Небор –Український блогер-лікар отоларинголог на дослідницькій позиції у госпіталі Цинциннаті, США. Засновник та керівник медичної платформи INgenius:

В інтерв'ю eHealth Іванка розповіла як працює електронна система охорони здоров'я в Америці та що особливого в роботі лікаря з eHealth в Штатах.

- Розкажіть, будь ласка, як функціонує електронна система охорони здоров'я в Америці.

В основному у великих лікарнях встановлена система «EPIC». Значна частина лікарів працює саме в ній. Проте, лікарі які відкривають власну практику та утримують невеликі лікарні, найчастіше не можуть дозволити встановити «EPIC». Вони обирають дешевшу програму. Ось до прикладу: 5 лікарів-лорів зібрались і відкрили свою приватну практику. З самого старту їм не вистачить коштів одразу купити «EPIC» і вони надають перевагу дешевшому варіанту.

- Хто в основному фінансує лікарські послуги в Америці?

Тарифи лікарів встановлюються виключно згідно їх спеціалізації і кількості випадків, які лікує певний лікар.

В більшості випадків все лікування пацієнтів здійснюється за страхуванням. Є різні види державного та приватного страхування. Ось програма державного субсидування Medicaid покриває дуже дорогі процедури. До прикладу кохлеарну імплантацію (операція, яку роблять при втраті слуху- встановлюють імплант, який замінює звуковий апарат). Але якщо якісь послуги не передбачені страховою виплатою пацієнта, їх можуть надати відповідно до окремого договору.

- Чи визначаються загальні правила та норми електронної медицини? Чи є якийсь орган який ними опікується?

Загальної основної структури, як міністерства тут немає. Але кожен штат встановлює свої певні правила ліцензування. До прикладу, під час пандемії дуже розвинулась телемедицина. Часто лікарі надають консультації колегам з інших регіонів. Але в тот час і виникли проблеми з впровадженням телемедицини, тому що кожен штат повинен надати ліцензію на цей вид послуг. Ось теледзвінок не можуть з Огайо провести в Каліфорнії, тому що лікарні, яка його проводить потрібно мати ліцензію на кожен штат.

- Хто обирає та встановлює електронну медичну систему в лікарні? Та як обслуговується дана система в лікарні?

Програму вибирає адміністрація. Це в основному не лікарі. Адже кожна лікарня в Америці – це окрема бізнес структура. Також обслуговують систему секретарі та відповідні менеджери. В Україні, як я проходила інтернатуру – зі страховими компаніями повинні зв'язуватися напругу лікарі або інтерни. В Америці ж усі фінансові питання, страхування, вирішують не медики, а відповідні фахівці. Лікар документує усі щоденики та описи хворих, але дуже мало займається організаційними моментами, оскільки це дорого дуже обійдеться лікарні.

- Чи долучаються приватні компанії до розробки функціоналу американського eHealth чи він лише державний?

Так, увесь функціонал в основному приватний. Взагалі, вважаю, що приватні інвестиції та структури – основа розвитку, будь-якої, медицини.

- Усі лікарі перед початком роботи проходять навчання з користування електронної системи охорони здоров'я?

В мене були тренінги в січні. Я записалася на курс. Збирається клас медичних працівників і кожен тиждень проводять навчання. Коли навчали працювати в системі, створювали окремих учнівський кабінет, де ми одразу могли спробувати використати весь необхідний функціонал. На самому початку стажування кожен обов'язково мав пройти тренінг з безпеки. На тренінгу пояснили усі правила роботи з програмою та захисту інформації пацієнтів. В Америці виділяється дуже багато часу та ресурсів для захисту приватної інформації громадян. Навіть після проходження курсу потрібно усі матеріали, що були роздруковані, викинути в окремих контейнер для утилізації, інакше можна отримати штраф.

- Які основні проблеми з якими зіштовхуються лікарі при роботі з системою?

Часто трапляються проблеми при передачі даних з різних медичних систем. Наприклад КТ, МРТ- це окрема електронна система. Якщо пацієнт зробив їх в лікарні, де немає договору з «EPIC», тоді або лікарня надсилає запит, щоб отримати знімки і це займає певний час, або пацієнт сам звертається в цей центр щоб отримати копію і на наступну консультацію приносить цей знімок. Але зачасту у великих університетських клініках завжди є свій діагностичний центр, де роблять КТ та МРТ.

- В системі «EPIC» ви зареєстровані, як «дослідник». Розкажіть, будь ласка, детальніше, що це означає та які є ролі в системі електронного здоров'я?

Для медиків це 3 основних позиції: лікар, медсестра і дослідник. В мене наразі позиція «дослідник». Кожна позиція має свій рівень доступу до медичних даних пацієнта. Коли входиш в систему- видно дані, які тобі доступні, але якщо є потреба в додатковій інформації, ти можеш надіслати запит і тобі підтвердять доступ до документів.

До прикладу: лікарю не потрібні щодня в користуванні форми медсестри, але якщо виникне потреба, в системі запитується доступ до файлу і після підтвердження він надсилається.

- Які заходи безпеки передбачені в системі?

Наразі, я працюю з дому і кожному, хто працює в системі, у лікарні видали окремих ноутбук для роботи в електронній системі з серійним номером та встановленими програмами захисту. Спочатку при його ввімкненні потрібно ввести логін і пароль, далі через попередньо встановлений спеціальний VPN додаток потрібно буде повторно ввести окремих логін і пароль. І при вході в саму систему «EPIC» вводиться ще одну унікальну пару логіна та пароля .

Коли безпосередньо працюєш з програмою в лікарні, потрібно здійснити лише вхід в систему «EPIC». Користувачі завжди повинні виходити з додатку. Не можна просто залишити комп'ютер з запущеною системою, тоді програма фіксує що ти в ній не працюєш, сама виходить і блокує доступ на декілька годин або на добу.

Одного разу в лікарні трапилось, що я не вийшла з облікового запису і цілу добу не мала доступу до системи.

- А пацієнти мають змогу безпосередньо взаємодіяти з системою?

Пацієнти мають свій окремий доступ до системи, де можуть подивитись на власні дані, а також за потреби мають змогу створити чат з лікарем. В Америці пацієнти зовсім не мають номерів лікарів і віддалено проконсультуватись з ними можуть виключно через систему.

- Як справи з інтероперабельністю систем: якщо пацієнт, змінить заклад, чи місце проживання, чи взаємодіють системи в закладах між собою і чи обмінюються даними про пацієнтів?

Пацієнт може отримувати будь-де лікарську допомогу, головне страховка, яка в нього оформлена. «EPIC» досі найпопулярніша система, в більшості клінік встановлена вона. Тоді зазвичай не виникає проблем, адже одна медична картка від народження в пацієнта і видно все від алергій які були в дитинстві до актуальних діагнозів. Немає випадків, коли пацієнт мав алергію, але забув про неї повідомити.

В емігрантів, які пізніше, а не з народження реєструються в системі можуть бути не всі актуальні дані, адже тут відповідно записується більшість інформації з їх слів.

- Є якісь особливості в роботі лікаря в Америці порівняно з українською практикою, які б хотілось відмітити?

В коментарях мені писали лікарі, що мають проблеми з функціонуванням eHealth в Україні. Що після роботи витрачають свій час, сидять і заповнюють все необхідне.

Звісно, ніхто не любить зміни і пристосуватись до нової роботи лікарю в будь-якому випадку важко.

В Америці теж лікарі закінчують свою зміну і залишаються заповнювати документацію. А паперової роботи ще більше ніж в Україні. Всім важко, ніхто не любить змін. Але всі звиклися і все буде добре! **(Як насправді працює eHealth в Америці // <https://ehealth.gov.ua/2020/10/06/yak-naspravdi-pratsyuye-ehealth-v-amerytsi-2>. – 2020. – 06.10).**

Центральный банк Эстонии Eesti Pank объявил о запуске исследовательской программы по созданию инфраструктуры цифровой валюты.

Согласно сообщению, Eesti Pank сотрудничал с технологическими компаниями SW7 Group и Guardtime для исследовательского проекта. Он направлен на то, чтобы увидеть, может ли решение блокчейна инфраструктуры подписи без ключа (KSI) запускать свою программу

виртуальной валюты. Эстония уже использует технологию блокчейна KSI для своих услуг электронного правительства. В рамках проекта банка будут также рассмотрены новые платежные решения, «которые станут возможными благодаря использованию электронных идентификаторов и других решений для электронного правительства Эстонии».

Однако в проекте не будет уточняться, какие технологии следует использовать.

Проект будет состоять из нескольких этапов и продлится около двух лет. На первом этапе будет изучено, как создать масштабируемую, практичную и безопасную платформу, отвечающую требованиям цифровых фондов. В то же время платформа также должна отмечать флажки скорости, безопасности, конфиденциальности и устойчивости.

Райнер Олт, руководитель отдела платежных систем банка, сказал:

«В качестве небольшого центрального банка Eesti Pank тщательно выбирает, в какие проекты развития центральных банков еврозоны мы можем внести значительный вклад. За прошедшие годы Эстония разработала уникальное ноу-хау о том, как поддерживать безопасное, частное и эффективное электронное правительство. Уникальный богатый опыт Эстонии дает хороший импульс для запуска проекта с технологическими компаниями SW7 и Guardtime для изучения технологических возможностей. Последний является долгосрочным партнером Эстонии по сотрудничеству в области блокчейна и абсолютным лидером в мире в этой области».

В банке подчеркнули, что они постоянно стремятся развивать финансовую среду и свою платежную систему, чтобы идти в ногу со временем и удовлетворять потребности граждан.

Эстония склоняется к технологии блокчейн, хотя ее программа электронного резидентства недавно подверглась критике из-за того, что электронные резиденты были связаны с мошенничеством.

В прошлом месяце президент Европейского центрального банка Кристин Лагард объяснила, что переход на цифровое евро не означает отказ от бумажных денег (*Виктория Ляпота Центробанк Эстонии проведет исследование цифровых валют // <https://cryptohamster.org/>* %D1 %86 %D0 %B5 %D0 %BD %D1 %82 %D1 %80 %D0 %BE %D0 %B1 %D0 %B0 %D0 %BD %D0 %BA- %D1 %8D %D1 %81 %D1 %82 %D0 %BE %D0 %BD %D0 %B8 %D0 %B8- %D0 %BF %D1 %80 %D0 %BE %D0 %B2 %D0 %B5 %D0 %B4 %D0 %B5 %D1 %82- %. – 2020. – 06.10).

Консалтинговая компания Boston Consulting Group (BCG) опросила более 700 руководителей компаний с оборотом более 500 миллионов долларов по всему миру, чтобы определить ожидания бизнеса в вопросе цифровой трансформации, а также подвести предварительные итоги работы по этому направлению в условиях пандемии; выяснилось, что пандемия COVID-19 «стала мощным катализатором цифровых трансформаций» по всему миру.

Среди лидеров цифровой трансформации – компании из сферы производства промтоваров (18 %); здравоохранения (16 %); IT, телекома, медиа (15 %); финансов (15 %).

Согласно результатам опроса, компании ищут решения с использованием цифровых технологий, которые будут способствовать работоспособности и восстановлению их бизнеса, позволят обеспечить широкомасштабное внедрение новых способов работы, защитят их системы от киберрисков, усилят возможности в области цифровой коммерции и маркетинга, а также позволят повысить автоматизацию операций и цепочек поставок.

Около трети опрошенных считают, что «цифра» уже сейчас имеет столь существенное воздействие на операции, что может изменить всю их бизнес-модель. Более 90 % участников уже ведут работу по цифровизации клиентской составляющей бизнеса, а более 70 % цифровой активности сейчас финансируется бизнес-подразделениями, а не технологическими.

BCG подчеркивает, что пандемия усилила интерес компаний к цифровой трансформации: 83 % компаний считает, что эта задача стала еще более важной, и около двух третей планируют увеличивать инвестиции в нее. При этом 80 % респондентов требует от программ цифровой трансформации самокупаемости, что в полтора раза выше, чем в 2017 году (около 50 % опрошенных) *(Коронавирус стал «катализатором цифровых трансформаций» – исследование // <https://d-russia.ru/koronavirus-stal-katalizatorom-cifrovyyh-transformacij-issledovanie.html>. – 2020. – 02.10)*.

Сведения о системах искусственного интеллекта, применяемых в столицах Нидерландов и Финляндии, приводятся на сайтах algoritmeregister.amsterdam.nl (Амстердам) и ai.hel.fi (Хельсинки), информация о самих реестрах опубликована на этой неделе.

Цель создания реестров и публикации их в открытом доступе – информировать граждан о применяемых в городах ИИ-системах и собрать отзывы о работе этих систем, сделать городские ИИ-системы «человекоцентричными». Разработку выполнила финская компания Saidot.

Реестры пока что содержат сведения о небольшом числе ИИ-систем. В Амстердаме действуют система управления парковкой; система сообщений граждан городским властям (пример сообщения – необходимость убрать мусор, ИИ-система сама пытается правильно адресовать такие сообщения); контроль соблюдения правил предоставления туристам жилья в аренду.

В Хельсинки ИИ-системы, вошедшие к настоящему времени в реестр, представляют собой чат-роботов, консультирующих, в частности, по вопросам парковки и о медицинских услугах. Одна из систем «заведует» библиотечным фондом, который совместно используется городскими библиотеками – ИИ контролирует и пытается оптимизировать перемещения книг.

И финны, и голландцы называют ИИ-системы «алгоритмами», что, строго говоря, неверно – системы искусственного интеллекта алгоритмическими не являются; эта терминологическая особенность закрепились, однако, в западных официальных документах и СМИ. Принципиальная проблема практического применения ИИ-систем состоит именно в том, что они не алгоритмичны, и в том, следовательно, что даже их разработчик не может ни объяснить результаты работы ИИ-систем, ни тем более контролировать их работу.

Поэтому публикация реестров ИИ-систем Амстердама и Хельсинки, попытка создания механизма общественного наблюдения за поведением искусственного интеллекта является важным событием – даже если единственным результатом будет привлечение внимания к названной проблеме (*Амстердам и Хельсинки первыми в мире создали реестры городских ИИ-систем // <https://d-russia.ru/amsterdam-i-helsinki-pervymi-v-mire-sozdali-reestry-gorodskih-ii-sistem.html>. – 2020. – 01.10*).

Новітня бібліографія зарубіжних та вітчизняних досліджень з проблематики електронного урядування

Ангел А. А. Електронне урядування у сфері державної реєстрації народження в Україні // Ефективність державного управління. – 2020. – № 63. – С. 75-87. Розглянуто основні організаційно-правові аспекти надання державної послуги щодо реєстрації народження. Значну увагу приділено особливостям удосконалення процедури державної реєстрації народження в Україні через запровадження веб-порталу та «пілотного» проекту «е-малятко». Досліджено специфіку застосування аналогічних моделей реєстрації у світі. Доведено необхідність подальшого удосконалення процедури запровадження інформаційно-комунікативних технологій у сфері реєстрації народження в Україні.

Дурман М. О. Електронні петиції як один з інструментів електронної демократії // Вісник Херсонського національного технічного університету. – 2020. – № 3 (74). – С. 131-139. В статті розкривається необхідність впровадження в державне управління інформаційно-телекомунікаційні технології (ІКТ), розвиток яких спричинює радикальні зміни в житті суспільства і пересічних громадян. Обґрунтовано, що однією з функцій державного управління та необхідною передумовою сталого демократичного розвитку є забезпечення прозорості та відкритості влади на всіх її рівнях. Саме це є запорукою здійснення ефективної політики, яка спроможна створити реальний громадянський контроль, забезпечити права людини та громадянина, зміцнити довіру громадян до влади. Досліджено, що найвищою формою електронного урядування є електронна демократія, яка дає можливість пересічним громадянам – членам суспільства брати участь у виробленні управлінських рішень. Це відбувається на всіх етапах процесу – від ініціації та розробки до прийняття та відслідковування результативності. Електронна демократія забезпечує нові форми комунікації, безперешкодний доступ до публічної інформації та сприяє участі громадян в виробленні і впровадженні державної політики. Громадяни використовують інструменти електронного урядування для взаємодії з органами публічної влади, а також для взаємодії між собою у питаннях політики та самоврядування. Доведено, що події останніх років демонструють прагнення громади до участі в ухваленні рішень. Спільнота налаштована на активніше застосування інструментарію залучення. Це ми можемо бачити на прикладі запровадження електронних петицій на рівні органів державної влади та місцевих рад. Цей інструмент запровадження е-демократії виступає як ініціатива демократії участі з боку громадян та підвищує мотивацію спільноти до застосування електронного урядування у взаємодії зі владою. На нашу думку майбутнє е-демократії полягає, насамперед, у використанні інформації та інформаційно-комунікаційних технологій в уже існуючих секторах демократії.

Жекало Г. І., Ключенко А. В. Програми інформатизації як складова механізму впровадження електронного урядування: порівняльна характеристика міст // Економіка, управління та адміністрування. – 2020. – № 3 (93). – С. 57-62. Ключовою складовою розвитку в системі публічного управління сьогодні є впровадження елементів електронного урядування на всіх етапах взаємодії владних структур з громадськістю. Одним із головних елементів електронного уряду є широка інформатизація суспільного життя, адже інформаційний ресурс у сфері

муниципального управління не менш важливий, ніж матеріальні, трудові, енергетичні, фінансові або інші ресурси. Тому головною метою статті є саме порівняльна характеристика програми інформування громадськості на місцевому рівні. Ми з'ясували, що головним методом інформування громадськості та забезпечення комунікації владних структур і населення є функціонування офіційних вебсайтів. Ми думаємо, що для визначення рівня відкритості та прозорості роботи того чи іншого органу влади найважливішими показниками є такі, як інформаційний контент інтернет-сайту, наявність елементів управління, можливість зворотного зв'язку, інтерактивність, доступність інформації різними мовами, наявність пошукових елементів сайтів, чітке групування повідомлень («хештегування»), відображення актуальної інформації не тільки на сайтах, але й на офіційних сторінках у соціальних мережах. У результаті дослідження ми зробили висновок, що вебсайти є офіційним джерелом інформування громадськості про минулі і майбутні події міста, дії влади міста, їх плани і перспективи. Водночас саме вебсайт є основним джерелом, який може забезпечити участь громадян у життєдіяльності міста. Сучасні версії офіційних сайтів міст спрямовані не тільки на інформування, а й на комунікацію з громадськістю, можливість отримання відповідей, коментарів, зауважень і пропозицій, враховуючи при цьому фізіологічні характеристики, особливості національності тощо.

Лебезова Э. М. Необходимость перехода к smart government как преодоление системных недостатков e-government // Век качества. – 2020. – № 3. – С. 30-46. В условиях пандемии новой коронавирусной инфекции Covid-19 резко вырос спрос на электронные государственные услуги, который выявил во многих странах несовершенство и ограниченность возможностей электронных правительств. В статье показано, что теория электронного правительства во многих случаях приходит в противоречие с практикой, что ведёт к серьёзным ошибкам, а также значительным финансовым потерям. Главный недостаток электронного правительства – использование устаревших организационных структур, моделей и процессов управления в новых форматах. В исследовании выявлено, что уровень коррупции в государственных структурах зачастую растёт с уровнем развития электронного правительства. Данный факт вызывает естественный скептицизм относительно эффективности таких реформ государственного управления. Цель статьи – показать неизбежность перехода от парадигмы e-Government к парадигме Smart Government, как более совершенной форме государственного управления. В центре внимания Smart Government находятся данные, что является главным преимуществом этой парадигмы перед парадигмой e-Government, которая акцентируется на бизнес-процессах и распределении ролей. К основным задачам работы можно отнести: выявление проблем связанных с цифровыми реформами государственного управления; описание главного отличия смарт-правительства от электронного правительства; разработка практических рекомендаций по совершенствованию процессов бесконфликтного перехода от электронного правительства к умному. Практическая значимость данного исследования состоит в том, что материал статьи будет полезен для независимой информационной экспертизы в области цифровизации органов власти и выработке мер для её трансформации в более совершенные формы.

Малик Е. Н., Шедий М. В., Пикалов Б. В. «Электронное правительство» как интегративная платформа предоставления государственных услуг // Управленческое консультирование. – 2020. – № 9 (141). – С. 19-30. В работе проведен комплексный анализ формирования «электронного правительства» в условиях развития нового государственного менеджмента. Выявлены факторы, влияющие на

становление и развитие электронного правительства. Авторами аргументирован вывод, что применение новых и совершенствование старых инструментов электронного правительства является важной задачей в контексте повышения эффективности системы государственного управления. Обоснованы преимущества развития интерактивного взаимодействия органов государственной власти и граждан через расширение деятельности госпорталов, МФЦ предоставления государственных и муниципальных услуг, а также государственных автоматизированных систем. Использование технологий и инструментов «электронного правительства» делает процесс государственного управления более открытым, так как граждане получают необходимый уровень информированности о результатах деятельности органов государственной власти.

Плахтій А. Бібліотечно-інформаційний супровід електронного урядування: українська практика // Бібліотечний вісник: наук.-теорет. та практ. журн.. – Київ. – 2020. – Вип. 1. – С. 14-22. У статті обґрунтовується важливість використання сучасного інформаційного потенціалу бібліотек для розвитку і популяризації інфраструктури електронного урядування, розкривається досвід вітчизняних бібліотек з надання державних електронних послуг фізичним та юридичним особам в умовах становлення електронного урядування. Висвітлюються основні теоретичні та організаційно-функціональні питання впровадження технологій електронного урядування у практику роботи публічних бібліотек.

Соанху Х. В., Папилина Т. М. Системный анализ проекта электронного правительства Республики Кот-Дивуар // ИТ-Стандарт. – 2020. – № 1 (22). – С. 25-30. Система предоставления услуг населению остается серьезной проблемой для Республики Кот-д'Ивуар. Крупные реформы, инициированные правительством, остаются в значительной степени незавершенными. В работе анализируется текущее положение реализации административной реформы и рассматривается разработка одного из проектов электронного правительства с учётом положений стандартов ИСО/МЭК.

Турдибеков Б. А. Приоритеты развития цифровой экономики и электронной торговли в Центральной Азии // Вестник Таджикского национального университета. Серия социально-экономических и общественных наук. – 2020. – № 4. – С. 116-121. Данная статья посвящена проблемам развития и современного состояния электронной коммерции в Центральной Азии. Цифровизация страны Центральной Азии – приоритетное направление деятельности. Цифровая трансформация представляет создание инновационных продуктов и услуг на базе комплекса передовых технологий. В зависимости от методологии и доступа к информации, данные, приведенные в этом материале, могут отличаться от данных других исследовательских проектов или государственных источников. Конечный итог принесет пользу правительствам и приведет к росту доходов населения, а также налоговых поступлений, которые можно будет использовать для социальных обязанностей государства. Действительно, прорыв, в первую очередь, должен быть направлен на повышение качества жизни людей стран Центральной Азии, это самая главная задача, всё остальное – вторично. Люди смогут выбирать тот образ жизни, который им наиболее интересен и важен, и строить такой мир, в котором они хотят жить. Все остальное, что мешает достигать человечеству устойчивого повышения качества жизни, должно уйти из нашего обихода. Например, такие явления, как терроризм, войны, коррупция, употребление и реализация наркотиков, а также алкоголь в Центральноазиатском регионе.

Ющенко Н. В., Базько О. А. Особливості трансформації електронного управління в сучасному суспільстві // Наукові перспективи. – 2020. – № 3 (3). – С. 75-71. Останні роки велика увага приділяється розвитку електронного урядування в країні. Розробляються нові електронні послуги, системи ідентифікації, нові платформи. В перше чергу електронне урядування дає змогу вдосконалювати адміністративні процеси, впорядковувати організаційний механізм публічного управління. Але досі немає чіткої взаємодії органів державної влади та місцевого самоврядування як по горизонталі так і по вертикалі. У світі відбувається трансформація урядування від електронного до цифрового та акцентується увага на користувачах послуг: громадянах, бізнес-структурах та громадських організаціях. Публічне управління стає все більш клієнтоорієнтованим. Відбувається зміщення центру уваги від інформатизації публічного управління до розвитку концепції інтелектуального управління. Визначено, що Україна в сфері розвитку електронного урядування на місцях займає не високі позиції і потребує дієвих механізмів розвитку регіонів. Ретельної уваги потребує запровадження цифрових трансформацій в містах. Від оцінки технічних можливостей та ІКТ інфраструктури до зручності та комфортності надання електронних послуг. Високої ефективності цифрових перетворень можливо досягти після розбудови детальної стратегії розвитку електронного міста, регіону з чітким визначенням механізму взаємодії усіх гілок влади. Розвиток інформаційного суспільства є пріоритетним напрямком розвитку країни в цілому, та в відповідності до європейських стандартів вимагає впровадження сервісно-орієнтованої державної політики. Тому вкрай важливо мати чітку стратегію розвитку країни в цілому, яка враховує особливості розвитку регіонів. Побудова стратегії впровадження електронного урядування та цифрового розвитку країни повинна починатися з оцінки ресурсів, які є в наявності, стикуватися з можливостями і напрямками розвитку регіонів та навпаки, розвиток регіонів повинен чітко інтегруватися в стратегію розвитку країни в цілому.