НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

ФАКУЛЬТЕТ СОЦІОЛОГІЇ І ПРАВА

МОДУЛЬНА КОНТРОЛЬНА РОБОТА

з навчальної дисципліни

«Наукові дослідження та форсайт в публічному управлінні»

Тема:

Розвиток e-урядування в Україні

Левицький Андрій СУ-31мп

Київ – 2023/2024

Зміст

1. Вступ

2. Розвиток електронного урядування в Україні

3. Сценарії

4. Висновки

5. Ключові події, Технології, Загрози, Нормативні акти

6.Список використаних джерел

Вступ

Електронне урядування є важливим інструментом для підвищення ефективності, прозорості та доступності державних послуг. В Україні розвиток електронного урядування став одним із ключових напрямів реформ, спрямованих на модернізацію державного управління та інтеграцію до глобального інформаційного суспільства. Цей процес включає впровадження цифрових технологій у роботу державних органів, автоматизацію адміністративних процедур та створення електронних платформ для взаємодії громадян з урядом. В умовах стрімкого розвитку інформаційних технологій та зростаючого попиту на зручні й швидкі послуги з боку громадян, електронне урядування в Україні набуває особливої актуальності. Таким чином, розвиток електронного урядування в Україні є комплексним процесом, який вимагає скоординованих зусиль держави, громадянського суспільства та міжнародних партнерів. Це не лише питання технічного впровадження цифрових сервісів, але й створення нового підходу до взаємодії між державою та суспільством, що сприятиме побудові прозорої, ефективної та демократичної.

Актуальність теми розвитку електронного урядування в Україні є безсумнівною та багатогранною. У сучасному світі, де цифрові технології швидко інтегруються в усі сфери життя, перехід до електронного урядування стає необхідністю для кожної держави, що прагне досягти високих стандартів прозорості, ефективності та доступності своїх послуг. По-перше, електронне урядування сприяє підвищенню прозорості та зменшенню корупції в державному секторі. По-друге, електронне урядування дозволяє значно покращити якість та доступність державних послуг. По-третє, розвиток електронного урядування сприяє активнішому залученню громадян до процесів прийняття рішень.

Розвиток електронного урядування в Україні

|  |  |  |  |
| --- | --- | --- | --- |
| **Тренди** | **Короткостроковий горизонт**  **До 5 років** | **Середньостроковий**  **10 років** | **Довгостроковий**  **Більше 15 років** |
| Збільшення кількості електронних державних послуг  -Цифровізація державних послуг: Швидкий перехід до надання більшості державних послуг онлайн. В Україні це проявляється через платформу "Дія", яка об'єднує десятки послуг на одному порталі.  -Інтеграція з іншими системами: Об'єднання державних систем та баз даних для спрощення доступу до послуг і покращення якості обслуговування громадян. | -Збільшення кількості електронних державних послуг: Очікується, що до 70% державних послуг буде надаватися онлайн, що значно полегшить доступ до них для громадян. | -Повна оцифровка державних послуг: Усі державні послуги будуть доступні онлайн, включаючи складні адміністративні процедури. | -Цифровий уряд: Перетворення уряду в повністю цифрову екосистему, де всі процеси автоматизовані та інтегровані. |
| Покращені технології розпізнавання громадян  -Біометричні дані: Використання відбитків пальців, розпізнавання обличчя та інших біометричних даних для безпечного доступу до послуг.  -Електронні ідентифікаційні картки: Впровадження ID-карток з біометричними даними для спрощення та безпеки ідентифікації. | -Покращені технології розпізнавання громадян: Впровадження біометричних технологій для ідентифікації особистості в онлайн-середовищі. | -Інтеграція штучного інтелекту: Використання штучного інтелекту для обробки даних та автоматизації державних послуг. | -Глобальна інтеграція: Інтеграція національних систем електронного урядування з міжнародними платформами для спрощення міжнародної взаємодії. |
| Збільшення кількості кіберзагроз  -Зростання кіберзлочинності: Підвищення активності хакерів та кіберзлочинців, які націлюються на державні інформаційні системи.  -Атаки на критичну інфраструктуру: Збільшення випадків атак на ключові державні системи, що може мати серйозні наслідки для національної безпеки. | -Порушення приватності: Збільшення кількості персональних даних, які зберігаються та обробляються державними установами, підвищує ризик порушення приватності громадян. | -Посилення кібербезпеки: Розробка та впровадження комплексних систем кібербезпеки для захисту державних інформаційних ресурсів. | -Кіберсвідомість громадян: Високий рівень кіберграмотності серед громадян, що дозволить ефективніше використовувати електронні послуги та захищати свої дані. |
|  | -Збільшення кількості кіберзагроз: Розширення онлайн-послуг супроводжується зростанням кіберзагроз, що вимагає вдосконалення кібербезпеки. | -Розширення правових рамок: Вдосконалення нормативно-правової бази, що регулює використання цифрових технологій у державному управлінні. |  |
|  | -Закон про кібербезпеку: Прийняття нового закону про кібербезпеку, що регулюватиме захист інформаційних систем та персональних даних. |  |  |
|  |  |  |  |

Сценарії

ПОЗИТИВНІ

-Повна оцифровка державних послуг: Громадяни можуть отримувати всі послуги онлайн, що значно економить час та ресурси.

-Високий рівень кібербезпеки: Надійний захист персональних даних та державних інформаційних систем зводить до мінімуму ризики кіберзагроз.

-Ефективне управління: Використання штучного інтелекту та великих даних для підвищення ефективності державного управління.  
НЕГАТИВНІ

-Порушення приватності: Масове збирання та обробка персональних даних можуть призвести до серйозних порушень приватності.

-Зростання кіберзагроз: Збільшення кількості кібернападів на державні інформаційні системи.

-Відсутність довіри: Громадяни не довіряють державним цифровим сервісам через побоювання щодо безпеки своїх даних.  
НЕЙТРАЛЬНІ

-Стабільний розвиток: Поступове впровадження нових технологій без значних ризиків або вигод.

-Регулярне оновлення законодавства: Прийняття нових нормативних актів відповідно до розвитку технологій, що забезпечує стабільність та безпеку.

Висновки

Позитивні сценарії

У випадку позитивного розвитку подій, загальнодоступність онлайн-послуг значно покращить життя громадян, забезпечуючи зручний і швидкий доступ до державних послуг. Ключовою подією стане широке впровадження платформи "Дія" та інших онлайн-сервісів, що об'єднають більшість державних послуг в одному місці. Використання передових технологій, таких як штучний інтелект, великі дані та блокчейн, дозволить підвищити якість та доступність послуг, зменшуючи корупційні ризики та підвищуючи ефективність роботи державних установ. Однак, для реалізації цього сценарію важливо постійно оновлювати технології та забезпечувати їхню безпеку, що вимагає значних ресурсів та компетенцій. Підтримку цього розвитку надаватимуть відповідні нормативні акти, що регулюють цифровізацію та надання електронних послуг. Високий рівень безпеки стане основою для довіри громадян до електронного урядування. Прийняття закону про кібербезпеку, який встановить високі стандарти захисту інформаційних систем, стане ключовою подією у цьому процесі. Впровадження передових рішень у сфері кібербезпеки, таких як багатофакторна автентифікація та шифрування даних, забезпечить надійний захист персональних даних та державних інформаційних ресурсів. Це зменшить ризики кіберзагроз та порушень приватності, що підвищить довіру громадян до цифрових державних послуг та стимулюватиме їхнє широке використання.

Негативні сценарії

У випадку негативного розвитку подій масові порушення приватності можуть стати серйозною проблемою, підриваючи довіру громадян до електронного урядування. Витоки персональних даних через неналежний захист інформаційних систем можуть спричинити значну шкоду громадянам та створити загрозу для національної безпеки. Постійні атаки на державні системи можуть призвести до порушення їхньої роботи, втрати даних та значних фінансових збитків. У таких умовах необхідно буде зосередити значні зусилля на вдосконаленні технологій кібербезпеки та розробці нових нормативних актів, які забезпечуватимуть ефективний захист даних.

Нейтральні сценарії

У нейтральному сценарії розвиток електронного урядування в Україні відбувається стабільно, без значних проривів або серйозних невдач. Цей сценарій передбачає поступове впровадження нових технологій та цифрових послуг з урахуванням наявних ресурсів і можливостей. Регулярне оновлення законодавства відповідно до розвитку технологій забезпечує правову основу для стабільного функціонування електронного урядування. Громадяни мають доступ до основних онлайн-послуг, але їхнє використання залишається помірним через обмежену довіру або недостатню інформаційну підтримку.Кібербезпека залишається на прийнятному рівні, без значних інцидентів або катастрофічних порушень, але і без значних інновацій. Законодавство розвивається поступово, враховуючи поточні потреби та виклики, але не завжди встигає за швидким розвитком технологій.

Ключові події

-Прийняття закону про кібербезпеку: Впровадження нового законодавства, що регулює захист інформаційних систем та персональних даних.

-Запуск порталу "Дія": Створення єдиної платформи для надання державних послуг онлайн.

-Впровадження біометричних технологій: Використання біометрії для ідентифікації громадян у цифрових сервісах.

Технології

-Біометричні системи: Розпізнавання обличчя, відбитків пальців, голосу.

-Штучний інтелект: Аналіз великих даних, автоматизація процесів.

-Блокчейн: Забезпечення прозорості та безпеки транзакцій.

Загрози

-Кібернапади: Постійна загроза з боку хакерів та кіберзлочинців.

-Порушення приватності: Неконтрольований доступ до персональних даних.

-Технічні збої: Можливі технічні проблеми та збої в роботі систем.

Нормативні акти

-Закон України "Про електронні документи та електронний документообіг" - Цей закон визначає правові засади використання електронних документів, їхню еквівалентність паперовим документам, порядок їхнього формування, обміну, зберігання та використання.

-Закон України "Про електронні цифрові підписи" - Цей закон встановлює правовий статус електронного цифрового підпису, його використання в електронному документообігу та інших сферах електронного урядування.

-Закон України "Про доступ до публічної інформації" - Він регулює доступ громадян до інформації, що належить до сфери публічного управління, включаючи електронний доступ до цієї інформації через веб-портали державних органів.

-Закон України "Про електронну ідентифікацію та електронні довірчі послуги" - цей закон визначає правовий статус електронних документів, електронних підписів та інших електронних довірчих послуг.

-Постанова Кабінету Міністрів України "Про затвердження Концепції розвитку електронного урядування в Україні" - цей нормативний акт визначає стратегічні цілі та завдання розвитку електронного урядування.

Список використаних джерел

1.Про схвалення Концепції розвитку електронного урядування в Україні. Єдиний веб-портал органів виконавчої влади України. URL: https://www.kmu.gov.ua/npas/250287124.

2.КОНЦЕПТУАЛЬНІ ЗАСАДИ РОЗВИТКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ В УКРАЇНІ. URL: https://ktpu.kpi.ua/wp-content/uploads/2016/02/Kontseptualni-zasadi-rozvitku-elektronnogo-uryaduvannya-v-Ukrayini.pdf.

3.Розвиток е-урядування: Кабмін затвердив процес електронної ідентифікації. LIGA ZAKON. URL: https://jurliga.ligazakon.net/news/224037\_rozvitok-e-uryaduvannya-kabmn-zatverdiv-protses-elektronno-dentifkats.

4.Чукут С. Тенденції та проблеми впровадження електронного урядування в Україні. URL: https://ktpu.kpi.ua/wp-content/uploads/2016/02/Tezi\_Tendentsiyi-ta-problemi-vprovadzhennya-elektronnogo-uryaduvannya.pdf.

5.ПРОБЛЕМНІ ПИТАННЯ РОЗВИТКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ В УКРАЇНІ. URL: https://www.niss.gov.ua/sites/default/files/2017-12/elekron\_vriaduv-26faf.pdf.

6.СУТНІСТЬ ТА ЗМІСТ ЕЛЕКТРОННОГО УРЯДУВАННЯ: КОНЦЕПТУАЛЬНИЙ ВИМІР. URL: http://www.dy.nayka.com.ua/pdf/8\_2020/54.pdf.