ЕЛЕКТРОННЕ УРЯДУВАННЯ В УМОВАХ КІБЕРЗАГРОЗ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Сідікі Олег Сайфуддін[1]

Опубліковано	Секція	УДК
30.01.2025	Публічне управління	35.072.8:004.738.5:004.056.5

DOI: https://doi.org/10.5281/zenodo.17254162

Анотація: Стаття присвячена аналізу проблем та перспектив захисту персональних даних у контексті електронного урядування в Україні. Розглянуто сучасні кіберзагрози, що впливають на роботу державних електронних сервісів, а також їхній вплив на довіру громадян до інститутів публічного управління. Проаналізовано конкретні кейси витоків даних, зокрема пов'язані із системою нотаріату та урядовими додатками, а також офіційні дані CERT-UA щодо кіберінцидентів у державному секторі. У статті окреслено нормативно-правові та технічні аспекти захисту персональної інформації, а також запропоновано шляхи підвищення кіберстійкості електронних систем та ефективності комунікацій між державою і громадянами. Результати дослідження можуть бути використані для удосконалення політики безпеки даних у публічному управлінні та розвитку електронного урядування в Україні.

Ключові слова: електронне урядування, персональні дані, кіберзагрози, інформаційна безпека, публічне управління, довіра громадян.

ELECTRONIC GOVERNANCE IN THE CONTEXT OF CYBER THREATS: PROBLEMS AND PROSPECTS OF PERSONAL DATA PROTECTION

Annotation. The current stage of development of the information society is characterized by the active introduction of digital technologies into all spheres of life, in particular into the sphere of public administration. In Ukraine, the process of digital transformation of the state has gained particular relevance after the introduction of electronic services and platforms that provide citizens with access to administrative services in a remote format. Electronic governance has become one of the key tools for implementing the principles of transparency, accountability and efficiency of government activities, as well as strengthening public trust in state institutions. At the same time, active digitalization generates new risks, among which cyber threats occupy a special place. Personal data leaks, cyberattacks on state registers and the spread of disinformation undermine citizens' trust in digital services and call into question

[1] *доктор філософії з спеціальності інформаційні системи та технології, доцент кафедри економіки підприємств та інформаційних технологій,*
ЗВО «Львівський університет бізнесу та права»
ORCID-ідентифікатор https://orcid.org/0000-0003-2586-7607

the effectiveness of the implementation of the concept of electronic governance. Recent information incidents, in particular around the notary system and allegations of data leaks from government applications, have demonstrated the need to rethink approaches to the protection of personal data and communications in the field of public administration.

The article is devoted to the analysis of the problems and prospects of personal data protection in the context of e-government in Ukraine. Modern cyber threats affecting the operation of state electronic services, as well as their impact on citizens' trust in public administration institutions, are considered. Specific cases of data leaks, in particular those related to the “e-Notariat” system and the “Diya” application, as well as official CERT-UA data on cyber incidents in the public sector, are analyzed. The article outlines the regulatory and technical aspects of personal information protection, and also suggests ways to increase the cyber resilience of electronic systems and the efficiency of communications between the state and citizens. The results of the study can be used to improve data security policy in public administration and the development of e-government in Ukraine..

Keywords: e-government, personal data, cyber threats, information security, public administration, citizen trust.

Вступ

Сучасний етап розвитку інформаційного суспільства характеризується активним упровадженням цифрових технологій у всі сфери життєдіяльності, зокрема у сферу публічного управління. В Україні процес цифрової трансформації держави набув особливої актуальності після запровадження електронних сервісів та платформ, що забезпечують доступ громадян до адміністративних послуг у дистанційному форматі. Електронне урядування стало одним із ключових інструментів реалізації принципів прозорості, підзвітності та ефективності діяльності органів влади, а також зміцнення довіри суспільства до державних інституцій.

Разом із тим активна діджиталізація породжує нові ризики, серед яких особливе місце займають кіберзагрози. Витоки персональних даних, кібератаки на державні реєстри та поширення дезінформації підривають довіру громадян до цифрових сервісів та ставлять під сумнів ефективність реалізації концепції електронного урядування. Нещодавні інформаційні інциденти, зокрема навколо системи нотаріату та звинувачень у витоках даних із урядових додатків, засвідчили необхідність переосмислення підходів до захисту персональних даних та комунікацій у сфері публічного управління.

Таким чином, дослідження проблем захисту інформації та забезпечення кіберстійкості електронних систем є надзвичайно актуальним завданням для України. У цьому контексті важливо не лише проаналізувати сучасні загрози, але й визначити перспективні напрями удосконалення механізмів захисту персональних даних, що стане запорукою подальшого розвитку електронного урядування..

Метою статті є дослідження проблем захисту персональних даних у системах електронного урядування в Україні, аналіз сучасних кіберзагроз та їхнього впливу на довіру громадян до публічних електронних сервісів, а також визначення перспективних напрямів удосконалення механізмів інформаційної безпеки та комунікацій у сфері публічного управління..

Результати

Аналіз сучасного стану електронного урядування в Україні демонструє, що впровадження цифрових сервісів державних органів супроводжується значними кіберризиками, які можуть ставити під загрозу персональні дані громадян. Зокрема, виявлені інциденти, зафіксовані CERT-UA, свідчать про системні проблеми у сфері інформаційної безпеки державних електронних платформ, що потребують комплексного підходу для їх вирішення.

Одним із найбільш резонансних випадків став інцидент з системою «е-Нотаріат» (CERT-UA №6282536), у результаті якого зловмисники отримали доступ до реєстру довіреностей, що містить персональні дані громадян [7,8]. Хоча Мінцифри запевняє, що інцидент не призвів до масштабного витоку, подія підкреслює реальні ризики компрометації інформації у державних реєстрах. Це свідчить про необхідність підвищення рівня захисту електронних сервісів, посилення контролю доступу та впровадження ефективних заходів моніторингу систем безпеки[7].

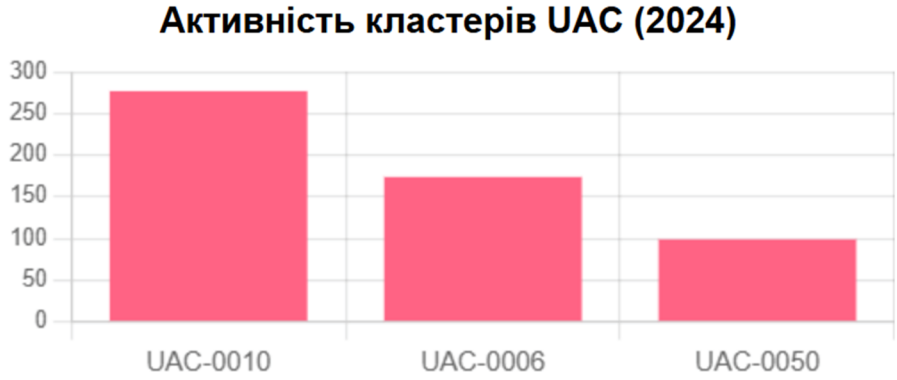

Рис. 1 Активність кластері UAC (2024)
Джерело: побудовано автором на основі [7,8]

У ході аналізу наданого витягу було виявлено цілу низку індикаторів компрометації, які свідчать про добре сплановану шкідливу активність. Знайдені файлові артефакти, специфічні командні рядки та мережеві адреси утворюють узгоджений набір доказів протифункціональної поведінки в системі.

Шкідливі файли розміщувалися в типових директоріях користувача (%APPDATA%, %LOCALAPPDATA%, %PUBLIC%) і додавалися до автозавантаження (Startup), що забезпечувало їхню постійну присутність у системі. Такі механізми persistence дозволяють зловмисникам зберігати доступ навіть після перезавантаження машини [7,8].

Виявлення RDP Wrapper свідчить про прагнення забезпечити постійний віддалений доступ до системи. Це класичний прийом для віддаленого контролю, коли атакуючі намагаються зберегти можливість підключатися до машини поза увагою користувача чи адміністратора.

Для початкового доступу та виконання завантажувальних модулів використовувалися стандартні утиліти Windows — mshta.exe, PowerShell та WMIC. Саме використання таких легітимних інструментів дозволяє атакуючим частково обходити захисні механізми й залишатися непоміченими довше.

Спостерігалася staged-схема завантаження: легкий початковий лінкер (наприклад, виклики mshta до віддалених URL) ініціює завантаження наступних, більш складних шарів шкідливої логіки. Приховані PowerShell-послідовності та закодовані блоки свідчать про застосування багаторівневого підходу, де статичні сигнатури виявляються менш ефективними через шифрування та степінг payload[7,8].

Мережеві індикатори (кілька IP-адрес і URL) формують чітку архітектуру C2-комунікації: наявність кількох адрес і портів дозволяє припускати розподілену інфраструктуру керування, а використання зовнішніх сервісів типу CDN/хостингу (наприклад, хмарне зберігання) допомагає маскувати джерела трафіку і забезпечувати надійну доставку компонентів.

Тактики і методи відповідають відомим категоріям у галузі кібербезпеки: запуск підписаних системних бінарників для виконання, виконання коду через PowerShell/WMIC, створення локальних облікових записів для забезпечення

персистентності та спроби обходу антивірусного захисту шляхом додавання виключень. У сукупності це характерно для кампаній зі середньою та високою мотивацією, що прагнуть прихованого і тривалого доступу.

З погляду виявлення, найбільш надійними сигналами є запуск mshta.exe з аргументами, які містять зовнішні URL; виконання PowerShell-команд з великими закодованими блоками або операціями AES-дешифрування; спроби додати глобальні виключення у Microsoft Defender; і поява несподіваних локальних облікових записів (наприклад, новий акаунт admin) [7,8].

Статичні сигнатури за окремими файлами мають обмежену ефективність через шифрування і поетапну доставку шкідливого коду, тому пріоритет слід надавати поведінковим індикаторам і мережевій активності. Моніторинг процесів, аналіз командних рядків і блокування підозрілих з'єднань дають більш надійний результат.

Для реагування найефективнішим виявився комплекс заходів: негайна ізоляція ураженого хоста і збір артефактів, блокування мережевих IOC як на периметрі, так і на самому хості, видалення артефактів персистентності та скасування небезпечних виключень у Defender. У разі підозри на глибоке ураження доцільно відновити систему зі свіжої, підтвердженої резервної копії, щоб мінімізувати ризик латентного збереження зловмисного доступу[7,8].

На довгостроковому рівні дослідження підкреслює необхідність впровадження EDR та розширеного логування (PowerShell, Sysmon), контролю або блокування запуску mshta.exe і подібних утиліт через AppLocker/SRP, регулярного аудиту автозавантажень і локальних облікових записів, а також підвищення обізнаності персоналу щодо фішингових векторів. Застосування цих контрзаходів істотно знижує ймовірність повторного успішного зламу за схожою схемою.

Приклади PowerShell-команд для збору даних :

```
# Список локальних користувачів
Get-LocalUser | Format-Table Name, Enabled, Description
# Перевірити Startup folder
Get-ChildItem "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup" -Force
# Перевірити конкретні шляхи
$paths = @("$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup\svchost.exe",
"$env:APPDATA\autoupdate.bat",
"$env:LOCALAPPDATA\RDPWInst.exe",
"C:\Program Files\RDP Wrapper\rdpwrap.dll",
"C:\Windows\System32\rfxvmt.dll",
"C:\Users\Public\Documents\bore.exe")
foreach ($p in $paths) { Write-Output "$p -> $(Test-Path $p)" }
# Показати виключення Microsoft Defender
Get-MpPreference | Select-Object ExclusionPath, ExclusionProcess, ExclusionExtension
# Швидкий netstat для перевірки з'єднань
netstat -ano | Select-String "87.120.126.48|89.105.201.98|193.233.48.166|194.0.234.155|91.92.246.18"
```

Інший важливий кейс стосується атаки на систему електронного документообігу одного з державних органів (CERT-UA №39606) [7,8]. Зловмисники здійснили кібератаку, що призвела до тимчасового припинення доступу до системи та потенційного витоку конфіденційної інформації [1,2,4]. Цей випадок показав, що державні органи недостатньо готові до організованих кібератак, а наявні механізми реагування на інциденти часто є неефективними. Він також демонструє значення

регулярного аудиту та оновлення систем безпеки для забезпечення безперервної роботи державних сервісів [1,7,8].

Рис 2. Розподіл подій ІБ за типами 2024 р.
Джерело: побудовано автором на основі [7,8]

Додатково, виявлені уразливості у системах електронного урядування (CERT-UA №6284080) свідчать про технічні недоліки, зокрема недостатнє шифрування даних під час їх передачі[7,8]. Подібні проблеми створюють можливості для перехоплення інформації та її несанкціонованого використання. Цей інцидент підкреслює необхідність застосування сучасних технологій захисту даних, включно з багаторівневою системою шифрування, багатофакторною аутентифікацією та сегментацією баз даних [7,8].

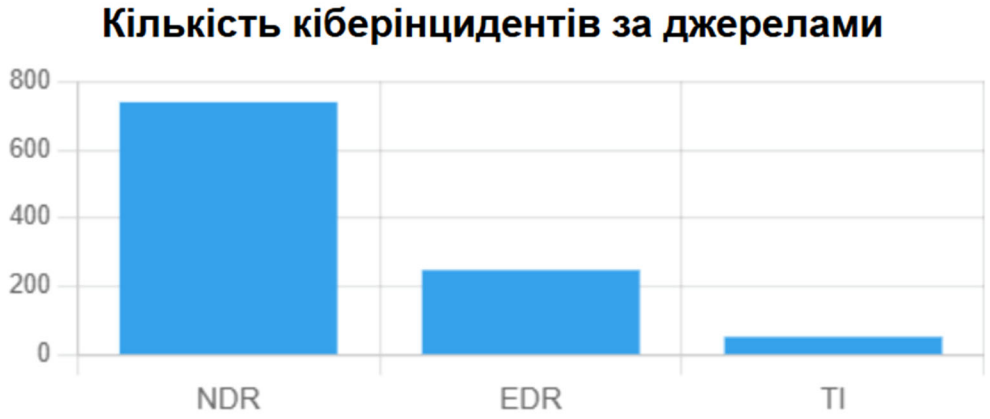

Рис 3. Кількість кіберінцидентів за джерелами 2024 р.
Джерело: побудовано автором на основі [7,8]

Загальний аналіз усіх розглянутих кейсів дозволяє зробити висновок, що електронне урядування в Україні стикається з комплексними викликами, які включають технічні, організаційні та комунікаційні проблеми. До технічних проблем належать застарілі або недостатньо захищені протоколи шифрування, відсутність багатофакторної аутентифікації та низький рівень контролю доступу до критичних баз даних[7]. Організаційні проблеми пов'язані з відсутністю регулярного аудиту систем, недостатнім рівнем підготовки персоналу та слабкими процедурами реагування на

інциденти. Комунікаційні виклики проявляються у низькій прозорості державних органів щодо заходів безпеки та недостатній інформованості громадян про механізми захисту їхніх персональних даних[2,4,5].

Таким чином, результати дослідження свідчать про необхідність комплексного підходу до захисту персональних даних у державних електронних системах. Це включає впровадження сучасних технологій шифрування, регулярний аудит систем безпеки, навчання персоналу, посилення контролю доступу та прозору комунікацію з громадянами [1,2,4]. Лише поєднання цих заходів дозволить підвищити довіру громадян до державних цифрових сервісів, мінімізувати ризики витоку інформації та забезпечити ефективне функціонування електронного урядування.

Висновки

У ході дослідження було встановлено, що електронне урядування в Україні стикається з комплексними кіберзагрозами, які створюють реальні ризики для безпеки персональних даних громадян. Аналіз інцидентів, зафіксованих CERT-UA, таких як витік даних через систему «е-Нотаріат», атаки на систему електронного документообігу та виявлені технічні уразливості в інших системах електронного урядування, свідчить про наявність суттєвих проблем у сфері захисту інформації [7,8]. Дослідження показало, що ключові проблеми пов’язані з недостатнім шифруванням даних, відсутністю багатофакторної аутентифікації, низьким рівнем контролю доступу, недостатнім моніторингом систем безпеки та слабкою підготовкою персоналу. Крім того, відсутність ефективної комунікації з громадянами щодо заходів захисту персональних даних сприяє зниженню довіри до державних цифрових сервісів. Узагальнення результатів дослідження дозволяє стверджувати, що підвищення кіберстійкості державних систем вимагає комплексного підходу, що поєднує технічні, організаційні та комунікаційні заходи[8]. До технічних заходів належать застосування сучасних протоколів шифрування, багатофакторної аутентифікації та сегментації баз даних. Організаційні заходи включають регулярний аудит систем, навчання персоналу та удосконалення процедур реагування на інциденти. Комунікаційні заходи передбачають прозору взаємодію з громадянами та інформування їх про заходи безпеки та політику захисту даних. Таким чином, ефективне електронне урядування можливе лише за умови постійного вдосконалення механізмів захисту персональних даних, підвищення обізнаності громадян та забезпечення прозорості державних сервісів. Впровадження таких комплексних заходів сприятиме підвищенню довіри населення до електронних платформ, мінімізації ризиків витоку інформації та розвитку стабільної та безпечної цифрової держави.

Список використаних джерел:

1. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Немкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. - Львів : Видавництво Львівської політехніки, 2019. - 580 с.
2. Комп’ютерні мережі : навч. посіб. / Т. І. Коробейнікова, С. М. Захарченко; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». – Львів : Вид-во Львів. політехніки, 2022. – 228 с.
3. Інтернет-технології опрацювання інформаційних ресурсів : навч. посіб. / А.М. Пелещишин, О. В. Марковець, Н. О. Думанський; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». – Львів : Вид-во Львів. політехніки, 2021. – 250 с

4. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.
5. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – Львів: "Магнолія 2006", 2024.-448 с.
6. Комп'ютерні мережі : навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. – Вінниця : ВНТУ, 2017. – 129 с.
7. Команда реагування на комп'ютерні надзвичайні події України — спеціалізований структурний підрозділ Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. URL:https://cert.gov.ua/.
8. Річний звіт Оперативного центру реагування на кіберінциденти URL:https://scpc.gov.ua/