https://doi.org/10.31891/2307-5740-2025-342-3(1)-1
УДК: 351.746.1:004.056

КУТОВА Марина
Національний університет «Чернігівська політехніка»
https://orcid.org/0009-0007-1693-7278
e-mail: dekfmip@gmail.com

МОДЕЛЬ СТРАТЕГІЧНОГО ПЛАНУВАННЯ РОЗВИТКУ СИСТЕМИ ЕЛЕКТРОННОГО УРЯДУВАННЯ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті запропоновано модель стратегічного планування розвитку електронного урядування в Україні, орієнтовану на забезпечення інформаційної безпеки. Доведено, що стратегічне планування із визначенням коротко-, середньо- та довгострокових перспектив є необхідним для комплексного вирішення сучасних викликів та ризиків, зумовлених розвитком інформаційного суспільства. Розглянуто основні завдання та заходи кожного етапу з акцентом на нормативно-правову базу, інституційну модернізацію, технологічні інновації, розвиток цифрової грамотності населення та міжнародну інтеграцію України у цифровий простір ЄС.

Ключові слова: електронне урядування, інформаційна безпека, кібербезпека, стратегічне планування, цифровізація, нормативно-правове регулювання.

KUTOVA Maryna
Chernihiv Polytechnic National University

A STRATEGIC PLANNING MODEL FOR THE DEVELOPMENT OF THE E-GOVERNMENT SYSTEM IN THE CONTEXT OF ENSURING INFORMATION SECURITY

The article proposes a strategic planning model for the development of e-government in Ukraine, with a central focus on ensuring information security. The research is motivated by the intensifying cyber threats accompanying digital transformation and the need for a coherent, staged approach to mitigating security risks in public administration. The author justifies the use of short-term, medium-term, and long-term planning horizons to structure the strategic response to current and anticipated digital vulnerabilities. In the short term, the focus lies on regulatory modernization, particularly aligning national data protection legislation with the EU's General Data Protection Regulation (GDPR), implementing the Cloud Services Act, and reinforcing human capacity through cybersecurity training for public servants. Institutional coordination is also emphasized, recommending the establishment of a permanent interagency cybersecurity body. The medium-term perspective targets the development of a secure and interoperable national digital infrastructure. This includes deploying certified national cloud systems, achieving full interoperability of government registries, enhancing digital identity platforms such as Diia, and finalizing the adoption and implementation of national AI and data protection strategies. A special emphasis is placed on building the operational capacity of cybersecurity institutions and fostering public-private-academic partnerships similar to those in Estonia and Israel. Long-term priorities involve embedding information security as a default feature of all e-government processes and transitioning to adaptive, AI-enhanced threat detection systems. The author calls for a dynamic legislative framework that can respond flexibly to technological evolution, participation in EU-level rulemaking bodies, and harmonization with European standards such as the EU Cybersecurity Certification Framework and eIDAS regulation. The vision culminates in Ukraine's full integration into the European Digital Single Market and the promotion of «digital democracy», wherein citizens are actively engaged in decision-making processes through open data and participatory digital platforms.

Keywords: e-government, information security, cybersecurity, strategic planning, digital transformation, regulation, digital identity, EU integration.

Стаття надійшла до редакції / Received 17.03.2025
Прийнята до друку / Accepted 26.04.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Зростання рівня цифровізації суспільства в Україні та стрімкий розвиток інформаційно-комунікаційних технологій супроводжується новими кіберзагрозами, що вимагає адекватного стратегічного реагування на державному рівні. Відтак, актуальною є проблема розробки стратегічних напрямів розвитку системи електронного урядування з інтегральним врахуванням аспектів інформаційної безпеки. Це питання набуває особливої важливості з огляду на необхідність формування послідовної, чітко структурованої та реалістичної політики, яка комплексно вирішуватиме сучасні проблеми інформаційної безпеки. Практичне значення проблеми полягає у необхідності створення моделі стратегічного планування, яка забезпечить чіткий розподіл завдань і ресурсів відповідно до коротко-, середньо- та довгострокових перспектив. Наукове значення полягає у розробці методологічно обґрунтованого підходу, який дозволить ефективно адаптувати державну політику до нових викликів цифрового середовища, встановити пріоритетність заходів, забезпечити ресурсну підтримку та готовність державних інституцій до реалізації заходів на кожному етапі.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Питання розвитку системи електронного урядування та забезпечення інформаційної безпеки активно досліджуються як вітчизняними, так і зарубіжними науковцями. Так, фундаментальні засади цифрового публічного управління та електронного урядування закладено у працях зарубіжних авторів, серед яких Хомбург В., Шолл Г. Й., Тройтіньйо Д. Р., Мазур В., Хьопман Й. Г., Фаунтейн Дж. Е., Норріс Д. Ф., Вест Д. М.Вони аналізують цифровий уряд як нову управлінську парадигму, проблеми цифрової довіри, застосування штучного інтелекту в адмініструванні та кібербезпеку. Серед українських дослідників значний внесок у вивчення проблематики інформаційної безпеки та модернізації публічного управління зробили С. М. Гнатюк, Л. С. Харченко, В. А. Ліпкан, О. М. Степанова, В. Н. Дереко, А. В. Велігура, О. Д. Довгань, М. П. Ільницький, С. А. Чукут, О. В. Загвойська, С. О. Гайдученко, І. Б. Жиляєв, А. І. Семенченко. Їх дослідження стосуються інформаційної безпеки, правового та інституційного забезпечення електронного урядування.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Попри існуючі напрацювання, недостатньо опрацьованими залишаються аспекти комплексного моделювання стратегічних напрямів електронного урядування в умовах війни, кіберзагроз та цифрової вразливості України. Відсутня цілісна модель імплементації міжнародного досвіду в українських реаліях, що враховує специфіку нормативно-правового регулювання, інституційної спроможності та технологічних можливостей держави. Подальші дослідження повинні бути спрямовані на формування інтегрованої моделі стратегічного планування електронного урядування з фокусом на інформаційну безпеку.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Запропонувати модель стратегічного планування розвитку системи електронного урядування в Україні з фокусом на забезпечення інформаційної безпеки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Доцільність застосування часових горизонтів у стратегічному плануванні розвитку електронного урядування випливає з необхідності комплексного вирішення проблем інформаційної безпеки, які різняться за пріоритетністю та ресурсною забезпеченістю. Короткострокові заходи (1-2 роки) націлені на оперативне вирішення гострих кіберзагроз та первинні регуляторні зміни. Середньострокова перспектива (3-5 років) передбачає комплексні реформи, узгодження з міжнародними стандартами та створення цілісної архітектури цифрових послуг. Довгострокова перспектива (понад 5 років) зосереджена на масштабних трансформаціях і формуванні стійкої інфраструктури цифрової безпеки, що забезпечить інтеграцію України у глобальний цифровий простір.

У короткостроковій перспективі пріоритетним завданням є оновлення нормативно-правової бази з метою усунення ключових прогалин у сфері цифрової безпеки. Насамперед це стосується вдосконалення регулювання у сфері захисту персональних даних. Зокрема, Закон України «Про захист персональних даних» [2] потребує гармонізації із положеннями Загального регламенту Європейського Союзу про захист даних (GDPR) [6]. Крім того, важливо забезпечити реальне впровадження положень Закону України «Про хмарні послуги» (2022) шляхом ухвалення відповідних підзаконних актів, які регламентуватимуть стандарти захисту інформації в державних хмарних інфраструктурах.

У найближчі 1-2 роки необхідно оновити національну стратегію розвитку електронного урядування, інтегруючи питання інформаційної безпеки в основу цифрових проєктів. Важливо застосовувати принцип «security by design», що передбачає вбудовану безпеку вже на початкових етапах розробки сервісів [5]. Приклад Сінгапуру та Данії свідчить про успішність такого підходу, де стратегія кібербезпеки тісно пов'язана з електронним урядуванням [5]. В Україні це вимагає синхронізації заходів з реалізації Стратегії кібербезпеки та цифрових реформ, забезпечуючи відповідні ресурси для впровадження нових стандартів інформаційної безпеки в державних установах [3, 4].

Особливу увагу слід приділити людському чиннику, який залишається однією з найвразливіших ланок у забезпеченні інформаційної безпеки. Тому необхідно запровадити обов’язкові навчальні програми для державних службовців, що охоплюватимуть основи кібергігієни, управління цифровими ризиками та навички безпечної роботи з конфіденційною інформацією.

Іншим критично важливим напрямом є забезпечення ефективної інституційної координації у сфері кібербезпеки в системі електронного урядування. У найближчі роки доцільним є створення постійно діючого міжвідомчого координаційного органу з питань цифрової безпеки та довіри. Серед його основних функцій мають бути: моніторинг кіберзагроз, реагування на інциденти, стандартизація вимог безпеки для державних ІТ-систем, а також узгодження дій між відповідальними відомствами. В Україні вже існують окремі елементи такої системи, зокрема Головний центр спеціального контролю при РНБО та команди CERT-UA. Проте наразі відсутній єдиний, централізований механізм управління цифровою безпекою. Тому доцільно інституційно консолідувати зусилля Міністерства цифрової трансформації, Держспецзв’язку, Служби безпеки України та

Національного банку України в межах єдиного координаційного органу, наприклад, на базі Національного координаційного центру кібербезпеки при РНБО. Такий підхід сприятиме швидкому обміну інформацією про загрози та формуванню цілісної політики кіберзахисту державних інформаційних ресурсів.

У середньостроковій перспективі стратегічним завданням є побудова інтегрованої цифрової екосистеми державного управління, у якій усі її елементи функціонують узгоджено, з дотриманням єдиних вимог до інформаційної безпеки. Це передбачає розгортання національної хмарної інфраструктури з підвищеним рівнем захисту, сертифікованої відповідно до міжнародних стандартів, таких як ISO 27001 [7], а також перенесення критичних ІТ-систем до надійно захищених дата-центрів.

Необхідно забезпечити повну технічну і функціональну взаємодію (інтероперабельність) між державними інформаційними системами з чітко визначеними правами доступу та безпечними протоколами обміну даними. Кожен запит до державної інформаційної системи має проходити перевірку, а всі сегменти мережі вважаються вразливими за замовчуванням [10]. Також у середньостроковому вимірі необхідно завершити імплементацію оновленого законодавства, Україна має ухвалити сучасний закон про захист персональних даних, узгоджений з вимогами GDPR, та створити незалежний наглядовий орган із забезпечення дотримання права на приватність.

Окремої уваги заслуговує розвиток інфраструктури електронної ідентифікації та довірчих послуг. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» вже створив правову основу [1], однак на практичному рівні необхідно її повноцінно реалізувати. Йдеться, зокрема, про розширення функціоналу платформи «Дія» як основного засобу цифрової ідентифікації особи. У цьому контексті доцільно впровадити національну програму цифрової ідентичності, яка забезпечуватиме надійну автентифікацію кожного громадянина при доступі до державних послуг.

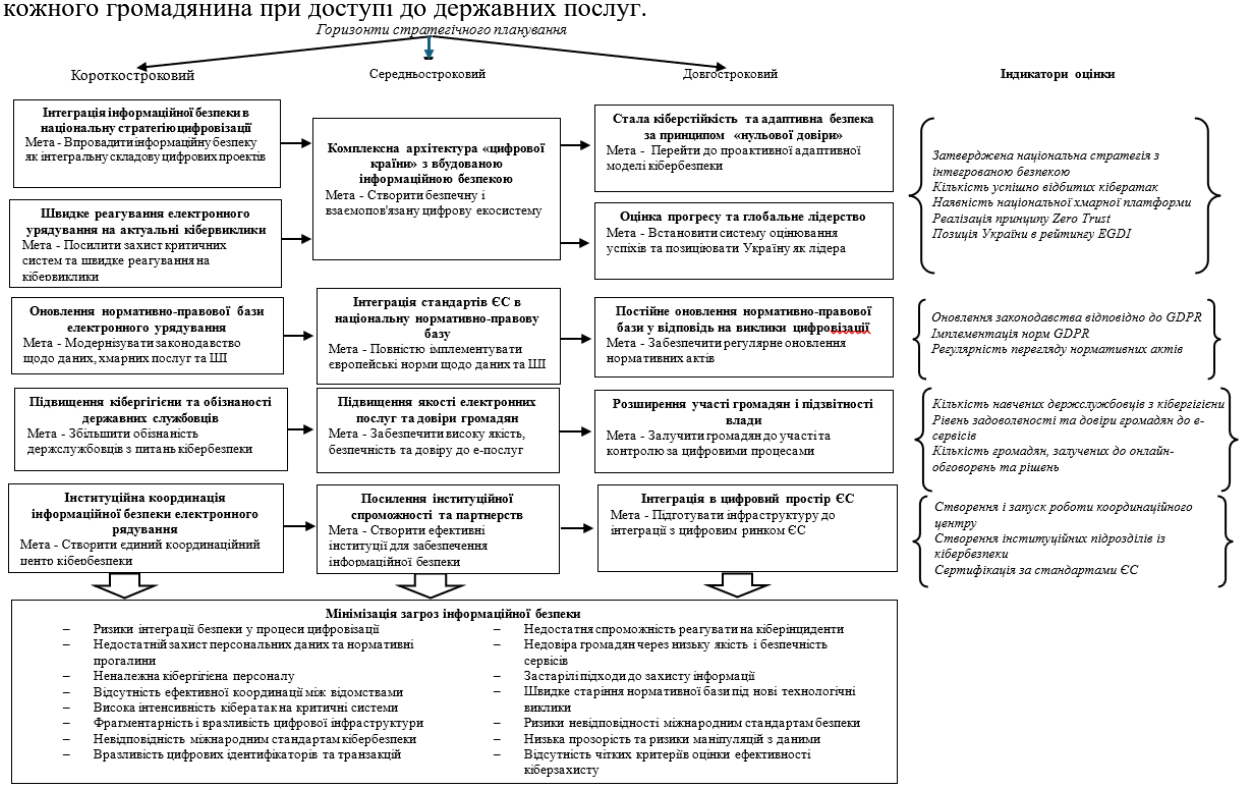

Рис. 1. Модель стратегічного планування розвитку системи електронного урядування в контексті забезпечення інформаційної безпеки

Ще одним середньостроковим завданням є забезпечення повноцінного функціонування новостворених інституцій у сфері кібербезпеки. Координаційний центр, створення якого передбачалося як пріоритет на першому етапі, має розвинути аналітичні спроможності, створити систему раннього виявлення загроз та механізми оперативного реагування. Усі державні органи повинні призначити відповідальних за інформаційну безпеку, які б координували свою діяльність з цим центром. До 2030 року Україна може ініціювати створення національного консорціуму з питань кібербезпеки за участі державних структур, ІТ-бізнесу та наукових інституцій.

У довгостроковій перспективі ключовою стратегічною метою є трансформація інформаційної безпеки в органічну складову всіх процесів цифрового врядування. Це передбачає перехід від реактивної моделі реагування на загрози до проактивної та адаптивної системи, здатної передбачати ризики та ефективно на них відповідати. Одним із пріоритетів є впровадження новітніх систем управління інформаційною безпекою (Security Information and Event Management) нового покоління, інтегрованих між усіма відомствами

та доповнених інструментами штучного інтелекту. Необхідно також забезпечити стійкість державної цифрової інфраструктури до перспективних викликів, зокрема квантових кіберзагроз.

З точки зору нормативного забезпечення, у довгостроковому горизонті має бути сформована динамічна та гнучка правова система, яка передбачає періодичне оновлення цифрового законодавства відповідно до технологічного розвитку. Для цього доцільно запровадити механізми регулярного аудиту правових актів, зокрема раз на 2-3 роки переглядати закони, що регулюють електронні інформаційні відносини. Україна має активно інтегруватися в європейські механізми вироблення цифрових норм, долучатися до робочих груп ЄС з питань ШІ, кібербезпеки та захисту персональних даних, аби заздалегідь готуватися до нових регуляторних вимог. Гнучкість законодавства також повинна дозволяти швидке врахування нових міжнародних угод та технічних стандартів. У звітах ООН за 2020-2024 роки наголошується на необхідності закріплення принципів безпеки, довіри та захисту прав людини як наскрізних складових цифрової трансформації [8,9,10]. Це має бути повністю відображено у правовій системі України, де базові права на приватність, захист даних і доступ до інформації фіксуються як непорушні незалежно від технологічного контексту.

Довгострокова стратегія також охоплює забезпечення громадянам і бізнесу України доступу до європейських цифрових сервісів: участь у публічних закупівлях в інших країнах, використання спільних платформ у сферах охорони здоров'я, освіти, соціального захисту. Це потребує не лише правового, а й технічного узгодження, зокрема, впровадження європейських стандартів інтероперабельності та підключення до пан'європейських цифрових інфраструктур. Отже, електронне врядування України повинно еволюціонувати від національної цифрової системи до невід'ємного елементу загальноєвропейського цифрового простору.

Нарешті, довгострокове бачення розвитку електронного врядування передбачає становлення моделі «цифрової демократії», де громадяни беруть активну участь в ухваленні рішень через цифрові канали. Урядові платформи мають забезпечити онлайн-дискусії важливих політик, прозорість у прийнятті рішень та систематичний громадський контроль. Регулярне оновлення відкритих державних даних повинно стати нормою.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Стратегічні напрями, визначені для коротко-, середньо- та довгострокового періодів, утворюють цілісну дорожню карту розвитку електронного урядування України з урахуванням ключових аспектів інформаційної безпеки. Вони органічно випливають із діагностованих викликів сучасного етапу, зокрема, вразливості державних реєстрів, недостатнього рівня суспільної довіри, фрагментарності нормативно-правового поля і спрямовані на досягнення стратегічної мети: побудови стійкої, безпечної та орієнтованої на потреби громадян цифрової держави. Успішна реалізація цих напрямів передбачає комплексну взаємодію між ключовими чинниками: підвищенням кіберстійкості, модернізацією законодавства, розвитком системи цифрової ідентичності, інституційними реформами та гармонізацією із нормами і стандартами Європейського Союзу. Такий підхід дозволить досягти необхідного балансу між впровадженням інноваційних цифрових технологій та забезпеченням високого рівня безпеки. Зростання довіри громадян до цифрових інструментів врядування стане природним результатом впровадження цих змін і визначальним чинником сталості цифрової трансформації. Адже саме довіра є основою ефективного функціонування електронного уряду та ключем до активної взаємодії суспільства і держави в умовах цифрової епохи.

Література

1. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII від 05.10.2017 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text
2. Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010 [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. План заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки України : затв. розпорядженням Кабінету Міністрів України від 19 грудня 2023 р. № 1163-р [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text.
4. Стратегія кібербезпеки України : затв. Указом Президента України від 26 серпня 2021 р. № 447/2021 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
5. Cybersecurity and Infrastructure Security Agency (CISA). Secure by Design [Електронний ресурс]. - Режим доступу: https://www.cisa.gov/securebydesign.
6. General Data Protection Regulation (GDPR) [Електронний ресурс]. – Режим доступу: https://www.consilium.europa.eu/en/policies/data-protection-regulation/
7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements [Електронний ресурс]. - Женева : International Organization for Standardization, 2022. - Режим доступу: https://www.iso.org/standard/27001.

8. United Nations. UN E-Government Survey 2020: Governing in the digital era [Електронний ресурс] / United Nations Department of Economic and Social Affairs. - New York: United Nations, 2020. - 258 p. - Режим доступу: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf
9. United Nations. UN E-Government Survey 2022: Governing in the digital era [Електронний ресурс] / United Nations Department of Economic and Social Affairs. - New York: United Nations, 2022. - 258 p. - Режим доступу: https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf
10. United Nations. UN E-Government Survey 2024: Governing in the digital era [Електронний ресурс] / United Nations Department of Economic and Social Affairs. - New York: United Nations, 2024. - 258 p. - Режим доступу: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024

References

1. Zakon Ukrainy "Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy" № 2155-VIII vid 05.10.2017 [Elektronnyi resurs]. – Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/2155-19#Text
2. Zakon Ukrainy "Pro zakhyst personalnykh danykh" № 2297-VI vid 01.06.2010 [Elektronnyi resurs]. – Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/2297-17#Text
3. Plan zakhodiv na 2023–2024 roky z realizatsii Stratehii kiberbezpeky Ukrainy: zatv. rozp. Kabinetu Ministriv Ukrainy vid 19 hrudnia 2023 r. № 1163-r [Elektronnyi resurs]. – Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text
4. Stratehiia kiberbezpeky Ukrainy: zatv. Ukazom Prezydenta Ukrainy vid 26 serpnia 2021 r. № 447/2021 [Elektronnyi resurs]. – Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/447/2021#Text
5. Cybersecurity and Infrastructure Security Agency (CISA). Secure by Design [Електронний ресурс]. - Режим доступу: https://www.cisa.gov/securebydesign.
6. General Data Protection Regulation (GDPR) [Електронний ресурс]. – Режим доступу: https://www.consilium.europa.eu/en/policies/data-protection-regulation/
7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements [Електронний ресурс]. - Женева : International Organization for Standardization, 2022. - Режим доступу: https://www.iso.org/standard/27001.
8. United Nations. UN E-Government Survey 2020: Governing in the digital era [Електронний ресурс] / United Nations Department of Economic and Social Affairs. - New York: United Nations, 2020. - 258 p. - Режим доступу: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf
9. United Nations. UN E-Government Survey 2022: Governing in the digital era [Електронний ресурс] / United Nations Department of Economic and Social Affairs. - New York: United Nations, 2022. - 258 p. - Режим доступу: https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf
10. United Nations. UN E-Government Survey 2024: Governing in the digital era [Електронний ресурс] / United Nations Department of Economic and Social Affairs. - New York: United Nations, 2024. - 258 p. - Режим доступу: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024