МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН, ІНФОРМАЦІЇ ТА РЕГІОНАЛЬНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувачка випускової кафедри
_____ Ніна РЖЕВСЬКА
«____»_____ 2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧКИ ВИЩОЇ ОСВІТИ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
СПЕЦІАЛЬНОСТІ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «КІБЕРБЕЗПЕКА СИСТЕМИ ЕЛЕКТРОННОГО ВРЯДУВАННЯ»

Виконавець: здобувачка вищої освіти 4 курсу, 409 Б групи, Павлюк Аліна Володимирівна

Керівник: старший викладач кафедри міжнародних відносин, інформації та регіональних студій Мазур Віра Іванівна

Нормоконтролер _____ Валентина ЄМЕЦЬ
(підпис)

КИЇВ 2022

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВРУ – Верховна Рада України

ЕУ – електронний уряд

ЄДРЮО – Єдиний державний реєстр юридичних осіб

ЄС – Європейський Союз

ІКТ – інформаційно-комунікативні технології

ІБ – інформаційна безпека

ІС – інформаційна система

КМУ – Кабінет Міністрів України

НАТО – Організація Північноатлантичного договору

ОБСЄ – Організація з безпеки і співробітництва

ООН – Організація Об'єднаних Націй

ОС – операційна система

ПБ – політика безпеки

ПЗ – програмне забезпечення

B2G – business to government, бізнес-держава

C2G – citizens to government, громадяни-держава

CIIP – Cisco International Internship Program, Програмf надійності та захисту ключової інформаційної інфраструктури

G2B – government to business, держава-бізнес

G2C – government to citizens, держава-громадяни

G2G – government to government, держава-держава

EGDI – E-Government Development Index, Індекс розвитку електронного уряду

ENISA – European Network and Information Security Agency, Агентство Європейського Союзу з питань мережевої та інформаційної безпеки

EPI – E-Participation Index, показник розвитку спілкування сервісів активної комунікації між громадянами та державою

OECP – Organisation for Economic Cooperation and Development, Організація економічного співробітництва та розвитку

OSI – Online Servise Index, широта та якість онлайн послуг

TII – Telecommunication Infrastructure Index, рівень розвитку комунікаційної інфраструктури

HCI – Human Capital Index, індекс людського капіталу

ВСТУП

Актуальність дослідження. Сучасний світ все більше потопає в технологіях. Звичні речі перестають мати свій первозданний вигляд. Багато що переміщується в настільки таємниче для більшості населення планети електронний простір, невидиме оку і невловиме, але настільки значуще для всього суспільства.

Його значущість бере свої витоки від зародження феномену інтернету, який придбав відомий нам образ лише в середині 1990-х років, привівши до колосального зрушення не тільки в галузі поширення та зберігання інформації, але й у сфері функціонування як приватних, так і державних інститутів. Інтернет, як загальнодоступна платформа, став першим кроком на шляху до віку інформаційних технологій. Все більше компаній і державних органів стало переходити на електронний документообіг, з кожним днем збільшуючи інтеграцію технологій у повсякденну рутину. Незабаром документообіг перестав бути єдиним завданням електронного простору, і на перший план вийшов термін інформація в його найбільш широкому розумінні, що включає все велике розмаїття матеріальних і нематеріальних людських благ, що переміщуються або знаходяться в електронному просторі.

Кібербезпека – це сукупність умов, за яких усі складові кіберпростору захищені від максимально можливої кількості загроз та впливів із небажаними наслідками.

Тепер інформація стала найбільш очевидним механізмом функціонування та двигуном еволюції громадських інститутів. Однак, з підвищенням рівня інтеграції у людства з'явилася не лише можливість прискорити темпи власного розвитку, а й виникли нові слабкі місця: виникла нова сфера, безпека якої, зважаючи на таку глибоку інтеграцію в людське та суспільне життя, вийшла на перший план для всього покоління. Загрози безпеки інформації та інформаційним ресурсам перейшли до розділу визначальних безпеку і свободу людини: підтримання конституційних прав на свободу та недоторканність, на захист гідності особистості та багато інших стало залежати від збереження порядку в інформаційному середовищі. Втім, вищезгаданий високий рівень людської інтеграції в це саме середовище вимагав більш чіткого

з'ясування області для взаємодії, тому був введений термін кіберпростір, що виступає сукупністю не тільки технологічних ресурсів інформаційного середовища, але і враховує прямий вплив людини на електронний простір.

Сучасний стан розвитку інформаційного простору характеризується новими потребами у створенні умов для безпечного функціонування його суб'єктів, коли особливо важливими стають проблеми протидії інформаційним війнам та захист власного кіберпростору. Тому актуальними питаннями, що розкриті в цьому модулі, є визначення основних понять, сутності та завдань захисту інформації, ознайомлення з Концепцією технічного захисту інформації в Україні, аналіз основних загроз інформаційній безпеці в системах електронного урядування (е-урядування) та вивчення основних методів протидії їм, що надає можливість використовувати отримані знання та навички на практиці.

Ця тема дозволяє отримати необхідні знання щодо основних понять, сутності та завдань захисту інформації та вміння щодо виявлення, запобігання й подолання найбільш поширених загроз інформаційній безпеці в системах е-урядування. Питання, що розглядаються у межах цього модуля, також пов'язані з іншими темами курсу, а саме: з проблематикою безпечного використання інформаційних ресурсів мережі Інтернет під час електронної взаємодії.

Метою даної роботи є опрацювання теми захисту інформації в системах е-урядування та безпечної роботи з інформаційними ресурсами корпоративних комп'ютерних мереж та мережі Інтернет.

Досягнення поставленої мети забезпечується виконанням таких **завдань**:

– охарактеризувати електронне урядування як основу управлінської діяльності державних установ;

– проаналізувати поняття кібербезпека як гарант безпечності впровадження систем е-урядування;

– охарактеризувати електронне урядування в Україні та подальші перспективи провадження.

Об'єкт дослідження – системи електронного урядування як невід'ємна складова сучасного суспільства.

Предмет дослідження – кібербезпека як основа впровадження електронного урядування в системи управління державою.

У даному дослідженні застосовувалися загальнонаукові теоретичні **методи**: метод відбору, узагальнення, аналізу та оцінки наукового матеріалу.

Практична значимість дослідження визначається тим, що розроблені узагальнені теоретичні та практичні матеріали, що містяться в роботі, можуть бути використані в організації освітнього процесу, спрямованого на отримання знань у галузі інформаційних технологій та захисту кіберпростору.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних інформаційних джерел. Загальний обсяг роботи складає 81 сторінка, з них основний текст складає 67 сторінок. Список використаних інформаційних джерел налічує 75 найменувань.

РОЗДІЛ 1. ЕЛЕКТРОННЕ УРЯДУВАННЯ ЯК ОСНОВА УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ ДЕРЖАВНИХ УСТАНОВ

1.1. Основні засади електронного урядування

До політичного та академічного дискурсів термін «електронний уряд» (ЕУ) увійшов наприкінці 1990 років. І досі немає однозначного тлумачення цього поняття, хоча існують трактування, запропоновані такими впливовими міжнародними організаціями, як European Commission (europa.eu.int, Європейська комісія), OECP (www.oecd.org, Organisation for Economic Cooperation and Development Організація економічного співробітництва та розвитку), World Bank (www.worldbank.org, Світовий банк) [2].

Європейська комісія дала наступне визначення поняттю «електронний уряд». Електронний уряд – це використання у державних структурах інформаційно-комунікаційних технологій на тлі проведення організаційних реформ та формування у державних службовців навичок, спрямованих на покращення функціонування держструктур та підвищення рівня послуг, які вони надають.

У 2001 р. Служба з питань державного управління OECP (Public Management Service) розпочала реалізацію проекту електронного уряду (e-government). Мета проекту – всебічний аналіз найпліднішого використання урядами інформаційно-комунікаційних технологій, що у свою чергу дасть змогу запровадити раціональні засади урядового управління. Основними характерними рисами даного проекту є: акцентування уваги на більш довготривалій та основоположній діяльності в галузі ефективного державного управління, реформа державної адміністрації. Електронний уряд визначений OECD як «використання інформаційно-комунікаційних технологій, і особливо Інтернет, як інструмент, що дозволяє досягти більш ефективного уряду» (from OECD The e-Government Imperative, 2003; OECD Електронний уряд Імператив, 2003) [11]. Такий інструмент дозволяє повніше реалізувати політику уряду, надавати якісніші послуги та підвищити рівень взаємодії з громадянами. Саме відповідно до цих критеріїв, що є запорукою успіху, надалі оцінюватиметься діяльність урядів та

інших державних структур. Ініціативи з налагодження електронного уряду фокусуються на низці таких проблем: яким чином організувати ефективнішу взаємодію різних структур з метою вирішення спільних проблем; як максимально враховувати інтереси споживачів; як створити міцні взаємини із партнерами з приватного сектора. Всі ці питання покликані вирішувати державні адміністративні органи [7].

В офіційних документах ООН термін «електронний уряд» українською мовою перекладається як електронні методи управління [22].

Серед відомих консалтингових компаній, які займаються дослідженням проблем електронного уряду, варто зазначити Accenture (Аксенчер), Gartner, Microsoft. Однак дані організації можуть бути зацікавлені у певному аспекті висвітлення поняття, що розглядається: з політичними цілями, комерційними, наприклад, продаж будь-якого програмного продукту [37].

Визначення ЕУ будуються фахівцями з різних принципів: описові прикладні, технічні, адміністративно-економічні визначення. Такі визначення відображають певні аспекти функціонування ЕУ:

– державне управління побудовано на основі використання електронних засобів обробки, передачі та розповсюдження інформації, надання послуг державними органами усіх гілок влади всім категоріям громадян;

– державне управління здійснюється за допомогою інформаційних технологій;

– присутність держави в Мережі;

– взаємодія органів влади та суспільства відбувається завдяки інформаційно-комунікаційним технологіям;

– для електронного бізнесу уряд постає одним з корпоративних користувачів інформаційних технологій;

– впровадження автоматизованих державних служб, що виконують наступні функції: забезпечують вільний доступ громадян до всієї необхідної державної інформації, збирають податки, реєструють транспортні засоби та патенти, видача необхідної інформації, укладання угод та оформлення постачання необхідних

державному апарату матеріалів та оснащення. Це дасть змогу значно зменшити витрати та зекономити кошти платників податків на утримання та фінансування діяльності державного апарату, зокрема рівень відкритості та прозорості діяльності органів управління збільшиться;

– органи державного управління впроваджують інтернет-технології;

– держава та громадяни взаємодіють за допомогою Інтернету [24].

Проте кожне з цих визначень представляє електронний уряд як новий підхід до покращення вже існуючих структур і відносин, ніж як самостійну ідею комплексної трансформації самих принципів організації управління державою.

Все різноманіття трактувань можна звести до двох груп. У межах першої дається поняття ЕУ у вузькому значенні, у межах другої – у широкому.

ЕУ у вузькому сенсі – це використання інформаційно-комунікаційних технологій у діяльності органів державної влади (надання послуг населенню та бізнесу, організації державних закупівель, здійснення фінансових операцій та надання інформації) [11].

ЕУ у широкому розумінні розуміється як процес трансформації внутрішніх та зовнішніх взаємодій у системах громадського управління, що забезпечується впровадженням інформаційних та телекомунікаційних засобів, з метою оптимізації управління, покращення якості обслуговування населення та забезпечення конституційних прав громадян [31].

Формування сучасної інформаційної та телекомунікаційної інфраструктури забезпечує:

– підвищення доступності електронних способів взаємодії з органами державної влади для організацій та громадян, зменшення часу, що витрачається населенням на взаємодію з органами державного управління;

– зниження витрат органів державного управління на надання державних послуг та виконання державних функцій в електронному вигляді;

– зниження витрат державного бюджету на виконання однотипних функцій загальнодержавної ваги завдяки централізованій їх реалізації;

– єдина технологічна платформа для оперативного захищеного інформаційного обміну між органами державної влади [40].

Віднесення будь-якої державної функції до інфраструктурної може бути повністю формалізованим і однозначним. Залежно від стадії зрілості формування електронного уряду, розвитку ринку та підвищення проникнення інформаційно-комунікаційних технологій у суспільство якісь раніше інфраструктурні компоненти можуть втрачати своє інфраструктурне значення, а якісь навпаки доцільно реалізовувати централізовано. Для усунення цієї принципової невизначеності, що не дозволяє приймати формальне рішення, чи належить конкретна державна функція та інформаційна система, що її підтримує, до інфраструктурної, у розділі сформульовані відповідні загальні принципи та критерії. Власне рішення мають прийматися та переглядатися на регулярній основі уповноваженим органом за регламентованою процедурою [33].

Базова класифікація інформаційно-технологічних та комунікаційних компонентів електронного уряду включає:

– відомчі та міжвідомчі прикладні (функціональні) інформаційні системи;

– інженерну інфраструктуру (телекомунікаційні та апаратні потужності);

– інформаційно-технологічну інфраструктуру електронного уряду (освічену сукупністю інфраструктурних інформаційних систем) [32].

Останні дві категорії (інженерна інфраструктура та інфраструктурні інформаційні системи) разом утворюють інфраструктуру електронного уряду, причому пріоритетну важливість і найбільшу складність складає формування інформаційно-технологічної інфраструктури (порівняно з інженерною). Це зумовлено тим, що інженерна інфраструктура виконує добре відомі, поширені та стандартизовані інфокомунікаційні функції, наприклад, надання каналів зв'язку на фізичному рівнях, надання доступу до Інтернету, інші мережеві служби та протоколи, формування локальних та територіально розподілених мереж, створення центрів обробки даних тощо. На відміну від неї інформаційно-технологічна інфраструктура повинна підтримати виконання повністю нових для країни функцій – насамперед

юридично значуща електронна взаємодія органів влади з громадянами та організаціями та між собою [34].

При цьому інформаційно-технологічна та інженерна інфраструктура електронного уряду компліментарна інформаційним та телекомунікаційним системам відомчого, регіонального та муніципального рівнів, а також інформаційним системам громадян та організацій.

Інформаційно-технологічна та комунікаційна інфраструктура електронного уряду не має самостійного значення, необхідність її формування обумовлена та обмежена завданням забезпечення віддаленої електронної взаємодії всіх учасників інформаційного суспільства. Надмірна концентрація (централізація) критично важливих компонентів на рівні інфраструктури несе у собі суттєві ризики, оскільки технологічно хибні рішення зроблять неефективною діяльність усіх учасників взаємодії. Тому якщо ті самі завдання можуть бути вирішені як шляхом ускладнення інформаційно-технологічної інфраструктури електронного уряду, так і доробкою функціональних (відомчих) інформаційних систем, у загальному випадку (за інших рівних) кращим є другий спосіб [3].

З цієї ж причини до інфраструктури електронного уряду не належать інформаційні системи, що забезпечують поточну діяльність органів державної влади (системи підтримки управлінських рішень, системи автоматизації поточної діяльності органів державної влади та місцевого самоврядування та ін.), хоча їхня роль та значущість для електронного уряду може бути близька до інфраструктурної (наприклад, ЄДРЮО) [13].

Для надання процедурі віднесення інформаційно-комунікаційних технологічних компонентів до інфраструктурного регламентованого характеру необхідно зафіксувати та закріпити нормативно наступний набір принципів:

– до інфраструктурних компонентів електронного уряду відносяться державні інфокомунікаційні системи, без створення та експлуатації яких забезпечення взаємодії державних інформаційних систем неможливе або економічно неефективне;

– функція, що підтримується інфраструктурою, повинна виконуватись одноманітно при вирішенні типових завдань, пов'язаних з електронною взаємодією

інформаційних систем електронного уряду, причому, не будучи реалізована централізовано, дана функція з неминучістю повинна виконуватись декількома органами державної влади або місцевого самоврядування (підрозділами одного органу). що призведе до непродуктивного дублювання неспецифічних органів влади функцій);

– якщо будь-яке інфраструктурне завдання може бути вирішене з використанням ринкових механізмів (без наділення органу влади новим обов'язком), то воно має виконуватися в опорі на ринковий механізм як із залученням бюджетного фінансування (оренда, аутсорсинг, закупівля), так і без. Прикладами інфраструктурних рішень, які може надати ринок, є пункти видачі сертифікатів цифрового підпису (приватні мережі УЦ), інфраструктурні засоби забезпечення доступу до сервісів електронного уряду (пошукові системи мережі Інтернет, комерційні центри обробки даних, телекомунікаційні потужності) та ін.

1.2. Етапи впровадження електронного урядування

Електронний уряд є складним комплексом засобів взаємодії між органами управління державою, громадянами та суб'єктами комерційної діяльності і передбачає три напрями взаємодії: G2B/B2G (government to business, держава-бізнес/бізнес-держава), G2G (government to government, держава-держава) та G2C/C2G (government to citizens, держава-громадяни/громадяни) – держава). Цей поділ умовно, оскільки найчастіше названі функції виконуються одними й тими самими електронними урядовими структурами. Але цілі у цих напрямів різні [40].

З розвитком G2B/B2G взаємодія між комерційними структурами та урядом полегшується за рахунок відкритого онлайн-доступу до законодавчої інформації (законодавчих актів, стандартів, інструкцій) та забезпечується можливість подання звітності до контролюючих держорганів через Інтернет.

Основне призначення G2G – покращити взаємодію між державними та місцевими органами влади, а G2C/C2G – забезпечити громадян зручним та швидким онлайн-доступом до інформації та послуг. Інакше кажучи, електронний уряд

відкриває доступ до нормативної правової інформації, а з іншого – дозволяє громадянам та комерційним структурам здійснювати різноманітні операції, починаючи від оплати комунальних рахунків та закінчуючи наданням звітності до держорганів, через Інтернет [43].

United Nations Division for Public Economics & Public Administration спільно з American Society for Public Administration виокремили наступні етапи розвитку електронного уряду:

– формується присутність держави в Мережі (emerging web presence): у країні з'являється один або кілька офіційних урядових сайтів, що надають користувачам статичну інформацію та службовців, що є інструментом зв'язку уряду з громадськістю;

– посилення присутності держави в Мережі (enhanced web presence): кількість урядових сайтів збільшується, надана інформація стає динамічнішою, при цьому користувачі отримують більше можливостей для доступу до державної інформації;

– присутність держави в Мережі стає інтерактивною (interactive web presence): здійснюється формальний обмін інформацією між користувачами та урядовими органами (заповнення форм, надсилання заяв онлайн);

– присутність держави у Мережі лише на рівні трансакцій (transactional web presence): користувачі мають легкий доступом до даних, пріоритетність яких визначається основі їхніх потреб; існують трансакції, що здійснюються онлайн (сплата податків, сплата реєстраційного збору та мит);

– цілком інтегрована присутність держави в Мережі (fully integrated web presence): інтеграція всіх державних інтернет-ресурсів є завершеною в рамках єдиного порталу [42].

На підставі міжнародних критеріїв, підготовлених Центром демократії та технологій, виділяються такі етапи розвитку електронного уряду, які наведено у таблиці 1.1.

Таблиця 1.1

Етапи розвитку електронного уряду

№	Найменування етапу	Опис присутності держави в Інтернеті	Опис етапу
1	Розміщення інформації	Базова присутність органів влади в Інтернеті. Не оновлюваний зміст сторінок - «візитні картки» державні [органів. Брошури з інформацією. Інформація для відділів зв'язків із громадськістю.	Створення сторінок міністерств та відомств, що містять інформацію про їх місію та напрямки діяльності. Сторінки держорганів зазвичай не підтримуються централізовано і не об'єднуються в єдиний портал.
2	Зворотній зв'язок	Комунікація з громадянами за допомогою електронної пошти – отримання довідок, інформації. Завантаження громадянами електронних форм для заповнення (податкові декларації, форми інших документів). Поповнення сайтів інформацією новин - перший елемент інформування про поточну діяльність держорганів.	З'являються перші елементи, інтерактивності (наприклад, відправлення питань та отримання відповідей громадян через e-mail); можна отримувати зразки деяких довідок та форм. Йде постійне оновлення новин щодо діяльності держорганів.
3	Транзакції	Взаємодія представників держорганів із громадянами у режимі реального часу. Здійснення деяких платежів за допомогою кредитних карток на сторінці уряду. Створення сторінок з аналогічними можливостями на міському та муніципальному рівнях.	Поява можливості здійснювати деякі операції в онлайновому режимі: сплачувати штрафи, замовляти паспортів, продовження дії деяких ліцензій та патентів. Така конкретизація роботи електронного правління, яка полягає вже не так в інформуванні, як в обслуговуванні. Для цього повинні бути створені

			спеціальні сайти для підтримки цих сервісів, як центральних, так і для міських і навіть районних органів влади.
4	Інтерактивні інтегровані послуги	Здійснення будь-яких видів платежів через портали центральних та регіональних органів влади. Поява регіональних порталів, що об'єднують державні послуги та послуги недержавного сектору.	Створення об'єднаних порталів різних відомств та служб, транзакцій, для здійснення яких раніше потрібно звертатися безпосередньо до цього. Завдяки регіональним порталам стає можливим зареєструвати підприємство, оформити фінансові документи, легалізувати іноземні документи тощо. З'являються регіональні портали, які поєднують у собі як весь спектр державних секторів – підключаються системи електронної комерції, інтернет-банкінгу.
5	Трансформація уряду	Створення електронної інфраструктури управління на основі єдиних стандартів. Урядовий портал як єдина точка доступу до всіх послуг – як громадянам, так бізнесу.	Створення електронної системи державного управління на основі єдиних стандартів, а також урядового порталу як єдиної точки доступу до всіх послуг – і для громадян, і для бізнесу.

Урядова веб-присутність (згідно з класифікацією Європейської комісії) характеризується послідовним проходженням п'яти етапів:

– інформаційний (Information). Уряд на 20% вважається віб-присутнім, цей етап включає в себе створення регулярно оновлюваних веб-сайтів, де публікується

основна урядова інформація, така як: нормативні акти, розпорядження, постанови та ін.). А також посилань на інші державні установи;

– інтерактивний односторонній (One way interaction). Уряд вважається веб-присутнім на 40%. На даному етапі прослідковується пасивна взаємодії між клієнтом та урядом. Мається на увазі надання послуг частково в режимі онлайн, проте з певним обмеженим функціоналом [7];

– інтерактивний двосторонній (Two way interaction) – 60%-ва веб-присутність. Реалізується за допомогою інтерактивної двосторонньої взаємодії. На цьому етапі онлайн сервіси стають інтерактивними і з'являється можливість запитувати інформацію щодо тих чи інших виступів та обговорень, звертатися до держчиновників електронною поштою, ставати учасником онлайн-дискусій або писати коментарі тощо [8];

– транзакційний (Transaction) передбачає 80%-ву веб-присутність. Основною характеристикою даного етапу є можливість надання послуг, що виконуються в онлайні на всіх стадіях. Прикладом може бути подання електронних заявок на отримання ліцензій на ведення професійної діяльності, подання податкових декларацій, заяв на обмін документів тощо. Проте, на даному етапі виникає серйозна загроза - забезпечення безпеки роботи [17];

– проактивний (Targetisation) – 100%-ва веб-присутність. Цей етап характеризується тим, що уряд може надавати не лише послуги обслуговування, а також залучає населення до прийняття рішень та двостороннього діалогу на базі інтерактивних сервісів.

У сфері інформаційних технологій, як і в будь-якій галузі соціальної активності, існують чотири види обмежуючих факторів: закони, ринок, норми моралі та архітектура. У цьому архітектура мережі, технологічні рішення ІКТ є у сенсі визначальними. Інакше кажучи, технологічні рішення завдань, які ставить уряд, можуть, своєю чергою, проводити зміст цих завдань [45].

При цьому процес розробки сайту стає не лише технічним, а й політичним завданням. Тому розробники повинні розуміти політичні наслідки ухвалення того чи

іншого архітектурного рішення. Важливою в цьому плані є класифікація сайтів різних поколінь, розроблена PWC Consulting (табл. 1.2).

Таблиця 1.2

Класифікація сайтів різних поколінь

	1-е покоління: Присутність в Інтернеті	**2-е покоління: Інструмент спілкування**	**3-є покоління: Взаємодія та транзакції**	**4-е покоління: Інтеграція ланцюжка**
Позиціонування	Створення сайту є самоціллю	Сайт – один із каналів інформування	Сайт – це інструмент для досягнення інших цілей	Модулі можуть бути також розташовані на інших сайтах
Політики	Практично не беруть участь	Зростання залучення/Складова IT	Оптимальне залучення / Окремий проект	Оптимальне залучення/Кооперація з ін.
Змістовне наповнення	Незмінна інформація (довідкова)	Інформація, що постійно змінюється (новини)	Інформація, взаємодія, транзакції	Інформація, взаємодія, транзакції
Технології	«HTML»	Бази даних/ Системи керування контентом	База даних, підключена до внутрішніх систем	Модулі, до яких також є доступ з сайтів ін.
Організатори	Ентузіасти	Департамент інформаційної політики	Профільні департаменти	Залучення спонсорів/ інвесторів/ зовнішніх партнерів
Політика є-уряду	Практично не пов'язані	Частина інформаційної політики	Є фундаментальною складовою держ. політики	Розділяється партнерами
Витрати	Незначні	Від $0,1 до $1млн	Понад $1 млн	Понад $1 млн

Електронна пошта	Ел. пошта надходить конкретному співробітнику	Пошта надходить на департамент чи централізовано	Пошта надходить у центр. вузол. Автоматичне розподілення	Пошта надходить у центр. вузол. Автоматичне розподілення
Моніторинг	Кількість відвідувань	Кількість відвідувань на сторінку	Запитання відвідувачів	Характеристика відвідувачів

1.3. Міжнародний досвід впровадження е-урядування в країнах світу

Сучасні концепції електронної держави здебільшого спрямовані на підвищення ефективності державного управління та підвищення якості надання державних послуг. З іншого боку, кожна країна, реалізуючи подібні програми, має свої власні цілі, зумовлені характером існуючих традицій та методик державного управління, внутрішньополітичними та геополітичними причинами, а також причинами культурного плану.

Проаналізуємо основні риси концепцій створення електронного уряду наступних країн: Австралія, Німеччина, Великобританія, США, Сінгапур, Фінляндія, Франція, Японія, Північна Корея, Китай.

Концепція розвитку інформаційних технологій Австралії (www.noie.gov.au) будується, виходячи з наступного принципу: інформація, якою можна управляти, становить національне надбання, яке має бути використане для оптимального розвитку політичної сфери та покращення роботи основних державних служб. Метою розвитку є досягнення такого рівня, за якого кожен австралієць зможе мати доступ до різних загальнодоступних інформаційних служб [43].

Наголошується на факті активного зростання електронної комерції – у середньому електронна торгівля дає 0,24 % відсотка економічного приросту, з 2000 року у доходах від експорту сильно зріс відсоток прибутку, отриманий від реалізації інформаційних продуктів [18].

Австралійський уряд ставить перед собою завдання інтеграції у глобальне інформаційне суспільство, поєднуючи для цього зусилля державних та приватних структур.

Розвиток технологій, які забезпечать можливість діалогу будь-якого громадянина країни з кожною організацією у світі, або з кожним громадянином будь-якої країни є пріоритетом на найближчі кілька років.

Розвиток інформаційних технологій та вступ у глобальне інформаційне суспільство розглядається авторами програми як доповнення до існуючих традиційних відносин, для їх удосконалення та подальшого розвитку [42].

Програма створення електронного уряду Сінгапуру («National Information Infrastructure and the realization of Singapore IT2000 initiative» www.informationr.net/ir/6-2/paper96/html), яка була сформульована у 2000 році, є стратегічною для цієї невеликої держави, в силу географічного положення та відсутності природних ресурсів. Спочатку урядом Сінгапуру було взято за основу програму інформатизації Японії та Євросоюзу [40].

Наголошується на важливості залучення до реалізації програми регіональної та місцевої влади та використання інформаційних технологій у комунальному обслуговуванні. Державні служби повинні стати ближчими для кожного громадянина, причому концепція обслуговування повинна бути єдиною для всіх жителів країни. Вкрай важливим є той момент, що передбачається інтегрувати електронні технології управління державою з аналогічними системами в Європі та Японії, що має позитивно вплинути на формування єдиного ринку та єдиної міжнародної політики. Активізація у громадському секторі має допомогти громадянам Сінгапуру отримати такі самі можливості, як і громадянам Європи та підштовхнути програму створення нових продуктів та послуг, які можуть бути реалізовані на глобальному ринку [18].

Для роботи на рівні місцевого самоврядування мають бути розроблені загальні закони, які зроблять громадську інформацію доступною для громадянина і забезпечать йому невеликий рівень витрат на її отримання. Автори програми вивчають вплив інформатизації на економіку та рівень зайнятості. Передбачається,

що вплив на рівень зайнятості виявиться позитивним через спрощення процесу навчання та перекваліфікації.

Програма державної інформатизації Німеччини (www.bund.de/nn_518/Content/BundOnline-2005/BundOnline-seite.html) говорить про те, що інформаційне суспільство принципово неможливе без електронного уряду [11].

Портал федерації є точкою централізованого доступу громадян до послуг та інформації органів управління Німеччини та інших громадських установ. Великими розділами є такі важливі події та теми, як, наприклад, Робота та професія, Будівництво, Пенсія, Економіка та наука, Управління та установи. Портал вважається складовою частиною ініціативи «Електронний уряд» федерації BundOnLine 2005. Крім федерації в проектах ЕП беруть участь землі та комуни. Для побудови інтегрованої системи у 2003 р. було прийнято рішення щодо реалізації спільної стратегії ЕП Deushland Online [17].

Список електронних державних послуг постійно розширюється, проте держава усвідомлює, що на даному етапі не можна не розвивати традиційні способи отримання державних послуг. Ключовою є ідея загального доступу до інформації державного управління, а також ідея оптимізації державних процесів, виключення подвійних дій та спрощення процесу отримання державних послуг.

Фінська програма створення електронної держави ставить глобальну мету: створення держави загального благоденства. Шляхом створення електронних урядових послуг може бути реалізовано такі можливості: забезпечення діяльності дослідницьких фондів, перерозподіл накопичень шляхом оперативних маніпуляцій прогресивним оподаткуванням та соціальним забезпеченням, а також підвищення ефективності систем комунального та соціального обслуговування. Отримавши ефективні механізми державного управління, уряд має сприяти підтримці національної ідентичності Фінляндії та входження до глобального інформаційного суспільства на загальних правах [35].

У програмі створення електронного уряду Великобританії («E-Government Unit. Focus of our work»: http://e-government.cabinetoffice.gov.uk) йдеться про те, що розвиток інформаційних технологій є основним фактором забезпечення ефективного

управління державою та постачання якісних комунальні послуги. Крім того, наголошується на важливості створення широкої інфраструктури електронного уряду в самій Великій Британії та інтеграція з урядами різних рівнів (на рівні ЄС, на рівні національних урядів та локальних органів влади). У програмі згадується, що фахівець з інформаційних технологій має відігравати важливу роль у діяльності уряду. За роки введення ЕУ у Великій Британії кількість державних службовців знизилася з 750 тис. (1976 р.) до 475 тис. осіб (2004 р.) [33].

Програма створення електронного уряду США (www.whitehouse.gov/omb/egov/about_backgrnd.htm) насамперед має на меті спростити та здешевити взаємодію громадян та представників бізнесу з державними структурами, а також уможливити пряме звернення громадян до уряду. Уряд США планує створити не представництва різних державних органів, а єдину інформаційну систему, яка охопить усі аспекти діяльності держави [45].

Програма створення електронного уряду в Японії реалізується на підставі прийнятої в березні 2001 року програми «317 кроків», головна мета якої до 2055 року забезпечити світове лідерство у сфері інформаційних технологій. Визначено п'ять пріоритетних напрямків: запровадження сучасних інформаційних мереж, використання інформаційних технологій в галузі освіти, розвиток e-commerce, застосування інформаційних технологій в адмініструванні та роботі соціальних служб та гарантування безпеки інформаційних мереж [45].

Французька концепція електронної держави розглядає інформаційні технології з погляду позитивних моментів, які можуть бути принесені завдяки їм діяльності держави. Вони повинні вплинути на рівень якості життя як у плані підвищення ефективності діяльності громадських служб, підвищення якості освіти та розширення ринку праці, так і на загальний економічний розвиток через спрощення доступу до світового ринку, збільшення конкурентоспроможності французьких підприємств та створення нових робочих місць у галузі електронних технологій. Особлива увага приділяється користі для національної культури, робота над образом Франції за кордоном, збільшення туристичної привабливості, надання Франції статусу культурного центру планетарного масштабу [45].

Таким чином, можна побачити, що французька концепція розвитку інформаційних технологій основним своїм завданням ставить завоювання Францією провідних позицій у різних галузях діяльності нового глобального інформаційного суспільства.

Перш ніж узагальнити цілі та завдання, які переслідують різні країни у формуванні структур електронного уряду, необхідно сказати про характерну для більшості країн-учасників процесу інформаційної глобалізації межі, а саме те, що серед цих країн переважають країни з федеративним державним устроєм. Другою характерною рисою є те, що через специфіку структури інформаційних технологій, у будь-якій точці планети може бути вирішена проблема централізації державної влади за умови великої територіальної протяжності держави та роз'єднаності регіонів. Третьою характерною рисою є прагнення країн-учасниць процесу забезпечити ефективність та доступність роботи центральної та місцевої влади. У той же час використання інформаційних технологій для загальнокультурних цілей здебільшого обмежуються освітніми та розвиваючими програмами. І, нарешті, загальною характерною рисою є прагнення держав, що розвивають електронні технології адміністративного управління, створити сумісну систему, яка дозволить рівним брати участь у процесі інформаційної глобалізації.

У 2001 році в Японії було оприлюднено стратегію «Електронної Японії» («e-Japan») [13]. Проект «Електронна Японія» передбачав створення спільноти, в якій кожен може активно користуватись інформаційними технологіями та усіма їх вигодами та перевагами. Уряд відігравав роль того самого середовища, в якому був би залучений приватний сектор. Ціллю «Елетронної Японії» було перетворення Японії в найрозвиненішу націю в світі в області інформаційних технологій. Основними напрямами «e-Japan» були:

- побудова ультра швидкісної мережі Інтернет та забезпечення доступом до мережі з будь-якої локаціях якомога швидше;
- розробка єдиних положень для e-commerce;
- реалізація концепції е-урядування;
- підготовка висококваліфікованих фахівців.

Після формування та затвердження стратегії потрібно було розробити план дій. «Програма пріоритетної політики електронної Японії» («eJapan Priority Policy Program») [11], «Програма побудови електронного уряду» («Program for Building E-Government») [16] стали цим механізмом. В основі даних програм лежали такі цілі: управлінські послуги, в першу чергу, повинні бути орієнтовані на користувачів та реалізація суспільного управління. Японії вдалось успішно надати громадянам та компаніям можливість подавати заяви і здійснювати реєстрацію фактично всіх національних адміністративних процедур. Станом на 2005 рік 96% національних адміністративних процедур були доступні онлайн. [15].

«Азійські тигри» (Південна Корея, Тайвань, Сінгапур і Гонконг) в основу свого інформаційного розвитку поклали модель економічного співробітництва держави і ринку. Великого успіху вдалось досягти завдяки втручанню держави в прийняття рішень, що стосується великих приватних капіталовкладень. Зокрема, завдяки активній участі держави в створенні національної інформаційної інфраструктури. Влада цих країн виокремлює наступні проблеми, що стають на заваді стрімкому інформаційному розвитку: зростання конкуренції в області виробництва, запровадження сучасних інформаційно-комунікаційних технологій, потенційна загроза втратити один з сегментів ринку чи робочі місця, а також проблема рівномірного доступу до інформаційних ресурсів.

Уряд Південної Кореї впроваджує е-урядування в рамках програми «Уряд для громадян» (G4C), основна мета якої полягає в спрощенні процедур взаємодії державних органів влади з громадянами та юридичними особами. Це планувалось досягти шляхом мінімізації прямих контактів владних осіб з громадянами країни та господарюючими суб'єктами. Для цього в країні було організовано електронний документообіг, що також включає усі питання оподаткування, а саме: оплата податків юридичними та фізичними особами за допомогою Інтернет, подання звітності юридичними особами, подання податкових декларацій фізичних осіб та надання податковими органами консультацій платникам податків в режимі реального часу.

Уряд Південної Кореї прийняв рішення щодо розробки інфраструктури і бази електронного уряду ще в 1987 році. За 35 років постійного вдосконалення систем е-

урядування населення країни мають змогу здійснювати всі операції, за виключенням деяких, лише за допомогою смартфона або ПК: починаючи від покупок в магазинах і закінчуючи оплатою рахунків і оформленням документів. По всій країні встановлено спеціальні термінали, які надають потрібну інформації та, навіть, можуть на місці роздрукувати будь-які довідки [25].

Південну Корею можна вважати не лише лідером по швидкості Інтернету, а й світовим лідером за ступенем охоплення широкосмуговою мережею населення.

В Китаї також, було прийнято схожий проект електронного уряду в 1999 році [39]. Через деякий час було запущено платформу на якій публікувалась громадська інформація та урядову мережу. Згодом спеціалісти створили інформаційні бази, які могли автоматично обробляти дані підприємств, населення та органів управління [7].

Шлях розвитку е-урядування, який пройшов Китай, можна умовно поділити на 3 етапи:

– стало можливим надання інформації і консультаційних послуг в режимі реального часу. Це означає, що громадяни отримують інформацію та послуги через Інтернет;

– надання публічних послуг онлайн. Цей етап характеризується тим, що громадяни мають змогу отримувати послуги в електронному вигляді;

– об'єднання онлайн послуг, тобто надання усіх можливих функцій на єдиній платформі (урядовий веб-сайт), що підпорядковується принципу «єдиного вікна) [22].

З моменту першого впровадження систем електронного урядування пройшло більше ніж країнам світу знадобилось більш ніж два десятиліття два десятиліття. Результатами постійних вдосконалень, спроб та досліджень є значна економія ресурсів (як матеріальних, так і часових), забезпечення населення високим рівнем надання послуг за допомогою онлайн-систем та підвищення ефективності функціонування органів державної влади. Все це – безцінний досвід, що може лягти в основу розвитку країн, що розвиваються.

РОЗДІЛ 2. КІБЕРБЕЗПЕКА ЯК ГАРАНТ БЕЗПЕЧНОСТІ ВПРОВАДЖЕННЯ Е-УРЯДУВАННЯ

2.1. Кібербезпека: суть та зміст поняття

Зародження Інтернету на рівні з появою аналогічних революційних технологій, на зразок колеса, велосипеда, літака, радіозв'язку та багатьох інших речей, призвело до якісного переосмислення людських можливостей з індивідуального та суспільного розвитку. Разом з приходом нових можливостей, як зазначалося, з'являлися й нові виклики безпеки людини. З цієї причини, зародження кіберпростору разом з появою Інтернету логічним чином викликало формування феномену кібербезпеки, як відповідь на виникнення загроз зовсім іншого характеру. Отже, для того, щоб виявити дійсну сутність терміна «кібербезпека», потрібно провести досконалий аналіз як явища кіберпростору, так і близьких до нього понять: інформаційної безпеки, інформаційного простору, кібератаки, кіберзлочинності, кібертероризму та деяких інших явищ [39].

Безумовно, формування подібного роду мережі, Інтернету, відбулося набагато раніше ніж у 1990-ті рр., однак, раніше ця технологія сприймалася як щось недоступне, оскільки проект формування єдиної системи моментальної передачі даних, який отримав грандіозну підтримку уряду Сполучених Штатів у 1960-і рр. XX століття, у період найбільш загостреного становища на світовій арені, призначався виключно для військового користування. Особливу роль у переході військового ресурсу у ранг загальнодоступного механізму зіграла передача технологій поширення інформації на руки наукового співтовариства європейської частини планети [5].

Ця подія відбулася саме на стику століть і кардинальним чином змінила уявлення людства про новоявлену мережу передачі даних, кількість користувачів якої значно зросла всього за кілька років: на початку 1990-х рр. XX століття було зареєстровано всього близько 20 тисяч користувачів мережі, у той час як на момент початку нового століття, у 2000 р. ця кількість зросла до 1 мільярда чоловік.

Інформаційна структура нового покоління не тільки набирала популярності серед громадськості, але й з кожним днем розширювалася, приймаючи на себе нові функції, що вийшли за рамки передачі інформації: зберігання, редагування, а також багато інших функцій стали доступні користувачам в онлайн-режимі в ході розвитку кіберпростору, проте кожну з них у кінцевому рахунку можна використовувати як на благо. Завдяки глибокій інтеграції політичних, соціально-суспільних, бізнес-структур в електронний простір, шкідливий вплив на їх дієздатність став однією з основних загроз, що виходять від інфраструктури кіберсередовища. Тоді експертною спільнотою всього світу почалося вироблення загальної школи трактування загроз і дій щодо їх запобігання у кіберпросторі, з метою розробки більш ефективних механізмів протидії шкідливим суб'єктам середовища [20].

Проте, вже на даному етапі експерти в галузі інформаційних технологій зіткнулися з деякими труднощами: у міру розвитку кіберпростору, середовище набувало все більш неоднорідного характеру. На відміну від інформаційного простору, що виступає сукупністю інформаційних ресурсів, впливаючих на них операцій з формування, зміни та поширення масивів даних, а також враховуючих області можливого застосування кінцевого продукту, поняття кіберпростору вимагало обліку кількох додаткових і при цьому непостійних суб'єктів, здатних впливати на фон: людини та техніку. Подібні суб'єкти, відмінною рисою яких виступає мінливість впливу на середовище, поряд з високим ступенем впливу, в кінцевому рахунку призвели до схожої з визначенням поняття тероризму проблематики, коли основний об'єкт вивчення не перманентний і неоднорідний, а тому не піддається точному трактуванню та включенню у правові та науково-детермініційні рамки [3].

Повертаючись до розгляду сутності поняття «кібербезпека», як уже було зазначено вище, міжнародній спільноті не вдалося дійти згоди у питанні загального сприйняття феномену. Проте експертні кола окремих країн все ж таки досягли деяких успіхів у даному напрямку, що безсумнівно сприятливо позначилося на методиці побудови національної безпеки з урахуванням нових викликів та загроз [37].

Наприклад, в американських академічних колах поняття кібербезпеки прийнято пов'язувати із сукупністю заходів, що проводяться, а також діючих у кіберпросторі інститутів, головною метою яких є захист національних інформаційних мереж, національних систем, що підтримують функціонування інфраструктури, і самої інформації від кібератак кіберсередовища. Подібний підхід обґрунтований прагненням до підтримки національної обороноздатності країни та знайшов відображення у прийнятих вищим військово-політичним керівництвом держави нормативно-правових актах. Наприклад, подібне трактування феномену кібербезпеки можна знайти в прийнятій у квітні 2015 р. Міністерством Оборони Сполучених Штатів Стратегії кібербезпеки, в якій також наголошується на захисті інформаційної інфраструктури Міністерства Оборони та необхідності гарантії безпеки мирному населенню країни [45].

Переходячи до розгляду позицій європейського експертного співтовариства, варто відзначити погляд турецького спеціаліста з безпеки М. Карамана на феномен кібербезпеки, представлений у науково-популярній статті під назвою «Institutional Cybersecurity from Military Perspective» або «Перспективи інституційного розвитку кібербезпеки для військових відомств» [8].

У своїй роботі автор підкреслює значущість створення не тільки технічних засобів захисту кіберсередовища, а й необхідність побудови багаторівневої системи національних інститутів, що забезпечують дієздатність кіберінфраструктури. Подібне становище походить від сприйняття самого явища кібербезпеки, що визначається фахівцем, як сукупність заходів захисту національного кіберпростору, що вживаються державою як у вигляді реакційних заходів, так і вигляді превентивних заходів, що поширюються як на кіберінфраструктуру, так і на навколишні суб'єкти. В даному випадку акцент робиться на значущість людського ресурсу, як визначальний загальний стан кібербезпеки [11].

Загалом позиції європейської експертної спільноти ґрунтуються на принципі «soft security», основою якого виступають положення про необхідність проведення «ненав'язливих» превентивних заходів щодо відсіювання суб'єктів, потенційно здатних виступити як загроза всій інфраструктурі. Таким чином, вкотре

наголошується на значущості людського фактора в стані кібербезпеки наших днів. На противагу цим міркуванням виступає принцип «hard power», основним «проповідником» застосування якого в кіберпросторі на сьогоднішній день виступає НАТО.

Організація Північноатлантичного договору, що виділяється як єдиний суб'єкт інформаційного середовища, приймаючи в січні 2008 р. Стратегію з кібероборони, як реакційні заходи, на події в Естонії, де серйозного удару зазнала кіберінфраструктура державних інститутів, вживаних урядами країн, міжнародним співтовариством та населенням планети, зокрема, заходів, спрямованих на захист індивідуальних, суспільних та державних кібернетичних систем, інформації та інформаційних ресурсів, розвиток національних та міжнародних механізмів боротьби з загрозами кіберпростору [2].

Таким чином, визначальним положенням сприйняття кібербезпеки з точки зору організації є необхідність обліку та побудови ефективної системи контролю та регулювання кіберсередовища, фактично виступає основним гарантом дієздатності феномену. При цьому, дотримуючись вищезгаданого принципу «hard power», основними механізмами забезпечення безпеки в досліджуваній галузі НАТО обирає звичні способи придушення ймовірних загроз, не заперечуючи можливості проведення самостійних операцій у кіберпросторі з метою знищення інфраструктурних компонентів, що становлять загрозу не тільки національній безпеці держав-членів, а також міжнародної кібербезпеці. Елементи побудови політики «hard power» організацією простежуються у чинній нормативно-правовій базі НАТО, де закладено основні засади функціонування суб'єкта [39].

На додаток до вищесказаного, слід зазначити, що об'єднаний центр передових технологій кібероборони НАТО у назві свого офіційного Інтернет-порталу, що містить визначення основних термінів пов'язаних з кіберпростором, зазначає, що позиція організації Північноатлантичного договору щодо детермінування самого кіберпростору та принципових діючих суб'єктів, виходить з узагальнення позицій, виражених у нормативно-правових актах держав-членів організації, а також враховує нюанси, вироблені науковим співтовариством за останні десятиліття, що дозволяє

створити успішнішу та прогресивнішу систему кібероборони, що охоплює всю широту області кібернетичної інфраструктури.

Тим не менш, не дивлячись на всі позитивні сторони вищезгаданих позицій зарубіжних фахівців та міжнародних організацій, у сприйнятті феномену з їхнього боку практично не приділяється увага правовому аспекту проблематики та впливу нормативно-правової бази сучасності на розвиток явища кіберсередовища [17].

Відзначаючи прогресивність поглядів академічного та військово-політичного співтовариства та узагальнюючи вироблені ними судження щодо сутності кіберпростору та кібербезпеки, формується єдина школа, що відображає сучасний стан феномена та вплив зовнішніх і внутрішніх чинників. Таким чином, з точки зору фахівців, феномен кібербезпеки являє собою безпеку суб'єктів кіберпростору, середовища, що включає не тільки технічні засоби, а й сукупність операційної взаємодії людини та програмного забезпечення, а також телекомунікаційні мережі, на просторах яких ця активність здійснюється, що досягається раніше всього прийняттям сукупності заходів щодо збереження стабільності та правопорядку в електронній інфраструктурі, підтримці дієздатності середовища в цілому, а також гарантують резистентність національних та міжнародних інститутів, інтегрованих у кіберпростір, виражених у вигляді формування суворої нормативно-правової, інституційної та технічної бази.

Іншими словами, сутність феномену виявляється у грамотній побудові сукупності базових елементів, що гарантують стабільність інформаційних інфраструктур. Як необхідна ремарка, яка надалі дозволить уникнути плутанини та виникнення певних розбіжностей, варто зазначити, що у вітчизняній нормативно-правовій базі поняття кібербезпеки та кіберпростору частіше підмінюються термінами інформаційна безпека та інформаційний простір, зберігаючи значення перших [4].

Виходить, що сприйняття феномену кібербезпеки у різних куточках планети безпосередньо пов'язане із виділенням основних суб'єктів кіберпростору. До таких суб'єктів можна віднести і правовий фон, розглянутий як один з базових елементів феномену кібербезпеки.

Крім того, темпи технологічного прогресу, що спостерігаються, змушують наукову спільноту замислитися про ефективність застосовуваних методів забезпечення безпеки в кіберпросторі. Одними з перших на зовсім інший шлях сприйняття кіберсередовища, як було зазначено вище, стали академічні кола, які впритул зайняли вироблення дієвих правових механізмів та їх просування в маси [22].

2.2. Основні засоби та методи захисту в системах електронного урядування

Практика впровадження систем електронного урядування в різних країнах світу існує понад два десятиліття. За цей тривалий період часу країни набули чимало досвіду. Якщо правильно його використовувати можна значно зекономити фінансові та людські ресурси, уникнути помилок, встановити єдині стандарти взаємодії національних систем електронного урядування з міжнародними [23].

Під час побудови сучасних систем з електронного урядування врахування досвіду різних країн світу у впровадженні систем е-уряду є надзвичайно необхідним. Основною проблемою під час впровадження електронного уряду були різні підходи щодо вирішення різного роду проблем.

Окрім цього, викликом для більшості країн світу стало несумісність інформаційних систем, що були створені у різні часові періоди, за різними стандартами та з різним технологічним забезпеченням. Робота систем електронного урядування побудована на основі інформаційних систем, що ґрунтуються на корпоративних комп'ютерних мережах [9].

Отже, на роботу систем е-урядування мають вплив проблеми, що характерні корпоративним структурами. Основними причинами, що призводять до виникнення таких проблем, можна віднести наступні.

По-перше, використання складного та різнорідного програмного та апаратного забезпечення. Для того, аби системи електронного урядування могли повноцінно виконувати усі завдання та функції для їх побудови використовують різні операційні системи. Найчастіше використовують операційну систему (ОС) Windows,

обробка інформації в системах електронного документообігу та важливі інформаційні ресурси зберігаються в базах даних, які знаходяться в ОС Linux, FreeBSD, Solaris.

З розвитком технологій та розширенням можливостей смартфонів державні службовці використовують мобільні пристрої з ОС Android та iOS. У даному випадку виникає інша проблема – технічне обслуговування пристроїв та проведення необхідних заходів у галузі інформаційної безпеки [6].

По-друге, велика кількість вузлів в системах електронного урядування. Через те, що вузли корпоративної мережі територіально розподілені, а часу для своєчасного контролю конфігураційних параметрів немає – виникає ще одна проблема [44].

До того ж однією з найважливіших проблем, що виникають в результаті використання систем е-урядування є долучення зовнішніх користувачів (тобто підприємств, організацій, окремих громадян) до відкритих сервісів і надання персоналу можливостей працювати віддалено з внутрішніми інформаційними ресурсами. А також збільшення загальної кількості факторів, до яких корпоративна мережа є вразливою.

Фактори, що впливають на ПЗ систем е-урядування можуть призвести до несанкціонованого доступу до інформаційних ресурсів. Саме тому вкрай необхідним є використання механізмів та засобів забезпечення безпеки.

Політика безпеки описує ці правила, закони та практичні рекомендації. Для забезпечення політики безпеки використовують наступні засоби: міжмережеві екрани; системи, що виявляють атаки; системи за допомогою яких можна шифрувати трафік; системи контролю «мобільного коду» (Java, ActiveX) та інші засоби [3].

Зокрема функціонування груп технічного обслуговування та інформаційної безпеки. Група технічного обслуговування займається переважно вирішенням питань, що стосуються системного та мережевого адміністрування.

До обов’язків групи інформаційної безпеки належать вирішення питань, що стосуються інформаційної безпеки на усіх рівнях (адміністративному, організаційному, технічному тощо).

Незважаючи на різній рід їх діяльності, все одно постає проблема розмежування їх функцій [25].

У Стратегії кібербезпеки України чітко визначені чинники, які можуть спровокувати виникнення загроз кібербезки, а саме:

– інфраструктура електронних комунікацій держави не відповідає належному рівню розвитку та захищеності сучасним стандартам;

– критична інфраструктура, державні електронні інформаційні ресурси недостатньо захищені від кіберзагроз;

– заходи для вдосконалення систем кіберзахисту не проводяться на регулярній основі;

– низький рівень розвитку організаційно-технічної інфраструктури забезпечення кібербезпеки;

– суб'єкти сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру працюють неефективно;

– взаємодія та інформаційний обмін між суб'єктами, що відповідальні за забезпечення безпеки кіберпростору знаходиться на низькому рівні [13].

У Стратегії національної безпеки України підкреслено, що загрози інформаційній безпеці складають ведення інформаційно-психологічної війни проти України, недостатність єдиної комунікативної політики держави та недостатній рівень медіа-культури суспільства. До загроз інформаційній безпеці відносять сукупність умов та чинників, що створюють потенційну загрозу інтересам суспільства, держави та особистості [11].

Загалом під загрозою інформаційній безпеці вважають «потенційно можливу подію, дію, процес або явище, які можуть призвести до нанесення шкоди системі». За більш деталізованим визначенням, загроза інформаційній безпеці системи – це можливість здійснення впливу на інформацію, що призводить до порушення конфіденційності, цілісності або доступності даних, а також можливість впливів на компоненти системи, які можуть призводити до втрати або знищення інформації чи збою функціонування ІС. Класифікація загроз інформаційній безпеці може бути здійснена за багатьма ознакам (рисунок 2.1).

Рис. – 2.1 Класифікація загроз інформаційній безпеці

Потрібно розглянути їх детальніше.

1. За природою виникнення:

Природні – це ті загрози, що виникли в результаті впливу на інформаційні системи певні дії фізичних процесів або стихійних природних явищ, що відбуваються незалежно від людини (природними загрозами можуть бути пожежі, повені, цунамі, землетруси, техногенні збої). Такі загрози складно, або, навіть, неможливо спрогнозувати.

Штучні загрози – такі, що викликані дією людського фактора [7].

2. За ступенем навмисності загрози:

Випадкові – виникають внаслідок халатності або ненавмисних помилок працівників. Яскравим прикладом є ненавмисне внесення помилкових даних або псування устаткування.

Навмисні – зазвичай виникають у результаті цілеспрямованої діяльності зловмисника. Приклад навмисної загрози – під час роботи з Web-інтерфейсом інформаційної системи на базу даних може бути використана атака за допомогою SQL-ін’єкцій з метою зміни або вилучення важливих даних [10].

3. Залежно від джерела загрози:

Загрози, які існують в природному середовищі. Приклади таких загроз – різке підвищення (пониження) температури атмосфери, геомагнітні аномалії, повені, буревії, інші природні катастрофи.

Загрози, джерелом яких є людина. Наприклад, влаштування недержавною організацією своїх довірених осіб, які діють в її інтересах, на посади, що займаються обслуговуванням державних ІС.

Загрози, джерелом яких є санкціоновані програмно-апаратні засоби. Як приклад – використання системних утиліт некомпетентними особами.

Загрози, джерелом яких є несанкціоновані програмно-апаратні засоби. Найбільш популярним є використання особистих носіїв (флешок, MP3- плеєрів, мобільних телефонів), що можуть містити віруси чи будь-яке інше шкідливе ПЗ [3].

4. За положенням джерела загрози:

Загрози, джерело яких розташоване зовні контрольованої зони. До таких загроз слід віднести наступні: перехоплення побічних електромагнітних випромінювань або перехоплення даних, що передаються каналами зв’язку; несанкціонована фото- і відеозйомка; перехоплення розмов, звукозаписів тощо.

Загрози, джерело яких знаходиться в межах контрольованої зони. Прикладами подібних загроз може бути застосування пристроїв для підслуховування або розкрадання носіїв, що містять конфіденційну інформацію [16].

5. За ступенем впливу на системи:

Пасивні загрози, які не прямого впливу ІС та не здійснюють ніяких змін у їх складі та структурі. Прикладом пасивної загрози може бути несанкціоноване копіювання файлів з даними.

Активні загрози. Реалізація активних загроз порушує структуру ІС. Наприклад, проникнення зловмисника до інформаційних ресурсів системи електронного урядування з метою моніторингу та перегляду вмісту мережевого трафіку для перехоплення паролів або інших важливих даних.

6. За способом доступу до ресурсів ІС:

Загрози зі стандартним доступом. Прикладом є несанкціоноване отримання пароля шляхом підкупу, шантажу, необережного зберігання, або фізичного насильства щодо законного власника.

Загрози, що використовують нестандартний шлях доступу. Приклад такої – використання незадекларованих можливостей засобів захисту.

До даної класифікації можна ще додати безліч загроз, проте найчастіше використовується класифікація загроз, яка ґрунтується на трьох згаданих раніше базових властивостях інформації (рис. 3), що захищається [6].

Варто відзначити, що реальні загрози інформаційній безпеці не завжди можна визначити за якоюсь конкретною категорією. До прикладу, загроза розкрадання носіїв інформації містить характерні риси усіх трьох категорій. Необхідно зазначити, що проблеми глобальної інформаційної безпеки посідають особливе місце в міжнародній інформаційній політиці та відображаються у звітах авторитетних організацій (ООН, ОБСЄ, ЄС та інші).

Відома Європейська агенція з питань мережевої та інформаційної безпеки («European Network and Information Security Agency», ENISA) була створена на початку 2004 р. з метою вирішення проблем, що пов’язані з вирішенням важливих питань у галузі інформаційної безпеки. Основні функції агенції – підвищення здатності європейських електронних мереж щодо протистояння зовнішнім впливам та атакам, збір та аналіз даних щодо комп’ютерних порушень в Європі та розробка методів оцінки й управління ризиками підвищення здатності ЄС реагувати на загрози в галузі інформаційної безпеки [35].

Стандарти інформаційної безпеки («Європейські критерії»), що розроблені у країнах Європи (Франція, Німеччина, Нідерланди та Великобританія) розглядають такі завдання інформаційної безпеки:

– інформація повинна бути захищеною від несанкціонованого доступу, аби не порушувати конфіденційність;

– захист інформації від несанкціонованих змін або, ще гірше – її видалення;

– системи повинні бути працездатними безперевно, тому важливо забезпечити їх роботу. Це здійснюється шляхом протидії загрозам відмови в обслуговуванні [31].

Для вирішення проблеми попередження загроз щодо ІС введене поняття гарантій механізмів захисту. Такі гарантії включають в себе:

– ефективність, тобто механізми, захисту повинні виконувати усі функції забезпечення безпеки;

– дотримання усіх стандартів під час їх розробки та правильність функціонування даних систем [35].

У «Європейських критеріях» нараховується сім рівнів гарантій: від Е0 до Е6 (у порядку зменшення ймовірності виникнення загрози). Рівень Е0 означає мінімальні гарантії (аналог рівня D «Жовтогарячої книги»). При перевірці гарантій аналізується життєвий цикл інформаційної системи – від початкової фази проектування інформаційної системи до експлуатації та супроводження. Рівні гарантій від Е1 до Е6 складені з наростанням вимог щодо ретельності та контролю. На рівні Е1 спеціалісти аналізують лише загальну архітектуру інформаційної системи, а функціональне тестування підтверджує гарантії механізмів захисту. На рівні Е3 вже більш детально тестуються вихідні тексти програм і схеми апаратного забезпечення. На рівні Е6 потрібен формальний опис функцій безпеки, загальної архітектури, а також політики безпеки, що забезпечують мінімальні ризики від загроз [4].

Таким чином, у «Європейських критеріях» визначені три рівні інформаційної безпеки – базовий, середній і високий. Інформаційна безпека є основною, якщо механізми захисту здатні чинити опір атакам та попереджати виникнення загроз. Інформаційна безпека вважається середньою, якщо засоби захисту здатні протистояти зловмисникам, що мають обмежені ресурси та можливості. Високою інформаційна безпека вважається, якщо засоби захисту можуть бути подолані лише злочинцями з високою кваліфікацією та з високим набором можливостей і ресурсів [42].

Необхідність захисту інформації від внутрішніх загроз історично була більш важливою на всіх етапах розвитку засобів інформаційної безпеки. З часом, на

внутрішні загрози, до яких відноситься витік інформації, стали звертати більше уваги. В основі витоку інформації полягає процес перенесення або передачі енергії чи речовини, які служать лише носіями інформації. За фізичною природою можливі такі шляхи переміщення інформації: світлові промені; звукові хвилі; електромагнітні хвилі; матеріали і речовини. Кожен переданий сигнал переноситься чи то за допомогою енергії, чи то речовин. Це може бути акустичні хвилі (звуки), електромагнітні випромінювання (світло, радіохвилі) або лист паперу (чи будь-який носій написаного тексту).

Використовуючи будь-яке фізичне поле, людина створює певну систему передачі інформації, що передається один одному. Їх називають системами зв'язку. Системи зв'язку складаються з джерел інформації, передавача, каналів, що передають інформацію та її одержувача. Ці системи широко використовуються відповідно до їх призначення і являють собою засоби передачі інформації [24].

Джерело інформації являє собою суб'єкта, яким створено певне повідомлення, звукові коливання, текст тощо. У джерелі сигналу ці повідомлення, як зазначено раніше, перетворюються в сигнали. Такі сигнали мають форму, що підходить для їх передачі каналами зв'язку. Канал зв'язку переносить сигнали з одного місця в інше до одержувача інформації. Витік інформації у розрізі розглянутого процесу передачі інформації розглядається як неправомірний вихід відомостей за межі системи передачі інформації.

Витік інформації також може здійснюватись за допомогою певного кола осіб, котрим деякі відомості були довірені. За своєю сутністю витік інформації означає протиправне (усвідомлене або випадкове, таємне або явне) оволодіння інформацією, що не має бути поширена, незалежно від того, яким шляхом її отримано.

Несанкціоноване зняття інформації з технічних каналів являє собою поширене явище. Такі канали витоку являють собою сукупність: небезпечних фізичних сигналів; середовищ розповсюдження та зберігання фізичних сигналів; об'єктів технічної розвідки; різні способи та засоби технічної розвідки. За результатами аналізу наукових робіт існує «узагальнена схема можливих каналів витоку і

несанкціонованого доступу до інформації, що обробляється в типовому одноповерховому офісі» [41].

Класифікація каналів витоку інформації також поділяється на:

– звукові канали витоку інформації;

– радіотехнічні канали витоку інформації;

– оптичні канали витоку інформації;

– речові канали витоку інформації, який визначається людським фактором [36].

Забезпечення інформаційної безпеки, в першу чергу, повинно здійснюватися на законодавчому рівні . Створення умов для безпечного використання інформаційно-комунікативних технологій, надання вільного доступу до інформації, захист від неправомірного доступу та витоку інформації повинно бути забезпечено законодавчими актами.

Що стосується питання захисту громадян, суспільства і держави від дезінформації та інших елементів інформаційної безпеки, то це також вирішується на законодавчому рівні. Під час створення нормативно-правового поля за основу беруться міжнародні, національні, галузеві нормативні документи та відповідні нормативні документи окремих органів публічного управління [34].

Безпековий фактор стосується усіх напрямів інформаційної політики України, що ви стосується чи не кожного з основних напрямів державної інформаційної політики України, що прописані в Законі України «Про інформацію»:

– кожен повинен бути забезпеченим доступом до інформації;

– кожен повинен бути забезпеченим однаковими можливостями щодо створення, збирання, отримання, зберігання, використання, поширення, охорони та захисту інформації;

– забезпечення в Україні належних умов для формування «інформаційного суспільства»;

– діяльність органів державної влади повинна бути відкритою та прозорою;

– постійне вдосконалення та розвиток систем е-урядування, а також створення нових ІС;

– безперервне оновлення, збагачення та зберігання національних інформаційних ресурсів;

– гарантування інформаційної безпеки України;

– посилення міжнародної співпраці в інформаційній сфері та входження України до глобального інформаційного простору [18].

Для впровадження та використання технологій інформаційної безпеки слід, в першу чергу, опиратись на Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Положеннями даного закону регулюються відносини у сфері захисту інформації. Також виокремлено хто є об'єктами захисту та суб'єктами відносин. Закон визначає порядок доступу до інформації; взаємовідносини між тим, хто володіє інформацією та користувачем; умови обробки та забезпечення захисту інформації; повноваження державних органів та відповідальність за порушення законодавства; міжнародні договори та прикінцеві положення [3].

Не менш важливим є Закон України «Про телекомунікації» у якому детально описано правове підґрунтя діяльності у галузі телекомунікацій та зазначено наступне:

– висвітлено повноваження держави стосовно управління та регулювання у сфері телекомунікацій;

– визначено права, обов'язки та відповідальності фізичних і юридичних осіб, які беруть участь у даній діяльності;

– права, обов'язки та засади відповідальності фізичних і юридичних осіб, які користуються телекомунікаційними послугами [22].

«Метою цього Закону є забезпечення повсюдного надання телекомунікаційних послуг достатніх асортименту, обсягу та якості шляхом обмеженого регулювання ринкових відносин для сприяння ефективному функціонуванню відкритого і справедливого конкурентного ринку. Закон визначає

засади захисту прав споживачів та контролю за ринком телекомунікацій з боку держави».

Закон України «Про Національну програму інформатизації» «визначає загальні засади формування, виконання та коригування Національної програми інформатизації, що також має включати безпекові аспекти».

Основними завданнями законодавства про «Національну програму інформатизації» стали: створити правові, організаційні, науково-технічні, економічні, фінансові, методичні та гуманітарні засади задля ефективного врегулювання процесу формування та впровадження цієї Програми та окремих її завдань (проектів). У «Національній програмі інформатизації» визначено стратегію за допомогою якої стане можливим вирішення проблеми забезпечення інформаційних потреб та підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної чи іншої діяльності у галузях загальнодержавного значення [40].

До складу Національної програми інформатизації входить:

- «Концепція Національної програми інформатизації»;
- державні програми з інформатизації;
- спеціалізовані програми та проекти інформатизації;
- програми та проекти інформатизації регіонального рівня;
- програми та проекти інформатизації органів місцевого самоврядування [41].

«Національна програма інформатизації» формується з урахуванням довгострокових перспектив соціально-економічного, науково-технічного, національно-культурного розвитку країни та ґрунтується на світових тенденціях розвитку у галузі інформатизації. Дана Програма повинна вирішувати найактуальніші проблеми, такі як: розвиток освіти, науки, культури, охорони довкілля та здоров'я людини, державного управління, національної безпеки та оборони держави та демократизації суспільства. Результатами впровадження Програми повинна бути інтеграція України у світовий інформаційний простір [34].

До Стратегії національної безпеки України, що була затверджена у 2015 р., входять наступні розділи: основні положення, завдання та цілі, фактори, що є

загрозою національній безпеці України, вектори державної політики, прикінцеві положення. Стратегією національної безпеки України визначено основні цілі:

– мінімізувати або усунути фактори, що загрожують суверенітету України та створити умови для відновлення територіальної цілісності держави в межах визнаного кордону у 1991 році, гарантувати мирне майбутнє для України та її громадян;

– затвердити права та свободи людини та громадянина, забезпечити ефективний розвиток економічної, соціальної та гуманітарної галузі, забезпечити інтеграцію України до складу ЄС та вступ в НАТО.

Серед інших проблем щодо актуальних загроз національній безпеці України, які мають бути вирішені, у Стратегії також зазначені:

– загрози інформаційній безпеці;

– загрози кібербезпеці та безпеці інформаційних ресурсів.

Зокрема, до загроз у сфері кібербезпеки та безпеки інформаційних ресурсів відноситься:

– незахищеність об’єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак;

– невідповідність систем охорони державних таємниць та іншої конфіденційної інформації сучасним стандартам [13].

Для ефективного вирішення проблеми забезпечення кібербезпеки та захисту інформації потрібно забезпечити наступне:

– інформаційна інфраструктура держави повинна постійно розвиватись;

– необхідно створити систему захисту від кібератак та розвивати мережу, що буде негайно реагувати на виникнення непередбачуваних ситуацій (CERT);

– своєчасне виявлення та прийняття належних дій для попередження та усунення можливих кіберзагроз;

– розширити можливості правоохоронних органів задля ефективного розслідування кіберзлочинів;

– максимально забезпечити усі об’єкти критичної інфраструктури від можливих атак та несанкціонованого доступу до них, повністю відмовитись від ПЗ, що було розроблено російськими спеціалістами;

– системи охорони держаної таємниці та конфіденційної інформації, системи е-урядування вимагають реформування враховуючи досвід країн НАТО та ЄС;

– забезпечити якісну підготовку професіоналів з питань кібербезпеки;

– посилити міжнародне співробітництво: Україна та НАТО і в рамках Трастового фонду НАТО [18].

Радою національної безпеки і оборони України у 2016 році було схвалено Стратегію кібербезпеки України. Дана Стратегія визначає основні положення, фактори, що загрожують кібербезпеці, національну систему кібербезпеки, пріоритети та напрями забезпечення кібербезпеки України, прикінцеві положення. Основною метою є забезпечити усі необхідні умови, що гарантуватимуть захищеність кіберпростору, виконання усіх його функцій в інтересах особи, суспільства і держави [45].

Пріоритетами проекту є:

– забезпечення стабільної роботи кіберпростору та його захищеність;

– надійний захист державних електронних інформаційних ресурсів та інформаційної та критичної інфраструктури від кібератак;

– надання необхідних повноважень та розширення можливостей сектору безпеки та оборони задля забезпечення кібербезпеки;

– боротьба з кіберзлочинністю [43].

2.3. Міжнародний досвід захисту від кібератак систем електронного урядування

Можна розглянути досвід Фінляндії у забезпеченні безпеки від кібератак систем електронного урядування. Відповідно до урядової програми, Фінляндія прагне стати однією з провідних країн світу за рівнем розвитку кібербезпеки. Проблемою

щодо розвитку Кіберстратегії, яку визначив Президент Фінляндії Саулі Нійністьо у 2012 р. є те, що в цій галузі необхідно постійно розвивати не тільки системи захисту інформації, а й досліджувати способи зламу даних. У зв'язку з цим у березні 2012 р. Фінляндія брала участь у координованих діях НАТО з військових навчань серед 20 країн альянсу на випадок виникнення кібервійни [2].

Така участь у військових кібернавчаннях є актуальною, через те, що за даними Відомства зв'язку у Фінляндії щорічно фіксується близько 250 000 різних порушень кібербезпеки. У розробленій у 2012 р. Стратегії національної безпеки та оборони Фінляндії один з основних розділів присвячений сфері інформаційної безпеки електронного урядування. У документі було зазначено, що проблема використання кіберпростору набуває все більш великого значення. Руйнування, які відбуваються в кіберпросторі, являють собою критичну загрозу національній безпеці Фінляндії.

До найбільш небезпечних причин виникнення кіберзагроз відносять вразливості, що знаходяться в корпоративних мережах. Наступною важливою причиною виникнення загроз є дії хакерів, які навмисно завдають шкоди або незаконно отримують інформацію (створюють витік інформації). Існує також досить суттєва частка виникнення випадкових збоїв у комп'ютерних мережах. У зв'язку з цим постає проблема розмежування кібератак і випадкових збоїв з метою визначення джерел загроз [17].

У Стратегії національної безпеки та оборони Фінляндії зазначено, що існують проблеми з різних питань у сфері кібербезпеки, що викликають конфлікт і розподіл думок в рамках міжнародного спільноти. Їх основними причинами стають інтереси економіки та безпеки, різні думки з питань прав людини і ролі держави в забезпеченні індивідуальної свободи. Ці питання вирішуються у співпраці з ЄС, НАТО, ОБСЄ і ООН, а також серед різних груп країн [36].

Також у Стратегії відзначено, що багато держав вдосконалюють свою здатність захищатися від кібератак і розробляють різні форми контрзаходів до зловмисників. Тому вирішення проблем виникнення та знешкодження кібератак є життєво важливими темами щодо національної та військової безпеки Фінляндії.

Стратегія кібербезпеки Фінляндії складається з таких розділів як вступ, бачення кібербезпеки, керування кібербезпекою та національний підхід, стратегічні принципи кібербезпеки, додатки (терміни та визначення). До бачення кібербезпеки Фінляндії належать такі положення:

– Фінляндія може забезпечити захист своїх життєво важливих функцій від кіберзагроз, що виникають у різних ситуаціях;

– громадяни, органи влади та бізнес-структури можуть ефективно використовувати безпечний кіберпростір і компетентності, які випливають із заходів кібербезпеки, як на національному, так і на міжнародному рівнях;

– Фінляндія запланувала глобальне лідерство в галузі усунення кіберзагроз і в управлінні наслідками, що викликані цими погрозами [24].

До основних рекомендацій, що записані в Стратегії кібербезпеки Фінляндії відносять:

– створення ефективної моделі співпраці між органами влади та іншими суб'єктами з метою розвитку національної безпеки та кіберзахисту;

– поліпшення всебічного розуміння ситуації кібербезпеки серед ключових дійових осіб в суспільстві;

– підтримка і розвиток можливостей підприємств і організацій, що грають вирішальну роль для виявлення та усунення кіберзагроз;

– надання відповідним органам необхідних заходів для запобігання, розкриття і усунення кіберзлочинності;

– визначення неодмінних умов для здійснення ефективних дій у сфері кібербезпеки в рамках національного законодавства [22].

Національний центр з кібербезпеки в Фінляндії містить інформаційні ресурси, що розкривають питання інформаційної безпеки, слабкі місця автоматизованих систем, практичні поради щодо забезпечення інформаційної безпеки різних організацій, права і обов'язки операторів телекомунікаційних вузлів.

Серед важливих розділів сайту: попередження, відомі уразливості, захищене використання послуг в галузі електронних комунікацій та застосування пристроїв

(ADSL-модемів, WLAN-пристроїв, міжмережевих екранів), електронні ідентифікаційні (цифрові підписи та сертифікати), інформація про інспекцію органів безпеки, права та обов'язки операторів зв'язку, права та обов'язки корпоративних абонентів зв'язку, статистика та звіти [17].

Ще один важливий інформаційний ресурс: Національний акредитаційний орган Фінляндії (FINAS) є національним органом з акредитації в Фінляндії. FINAS акредитує лабораторії, органи з сертифікації, інспектуючі державних органів, фахівців з професійного тестування і перевірки параметрів навколишнього середовища та викидів парникових газів. Серед важливих розділів сайту є новини, цікаві статті, відомі курси, різні послуги, інформація про акредитації тощо.

Міністерство фінансів Фінляндії також приділяє велику увагу питанням кіберзахисту наявних інформаційних ресурсів держави. У матеріалах, розміщених на сайті Міністерства фінансів Фінляндії зазначено, що існують загальні відправні точки, які включають в себе відповідальність кожної організації в галузі інформаційної безпеки під час здійснення своїх власних операцій, зобов'язання з інформаційної безпеки, передбачені нормативно-правовими актами, Постановами Уряду про підвищення інформаційної безпеки Фінляндії, Стратегією кібербезпеки Фінляндії, а також інструкціями з інформаційної безпеки, виданими Міністерством Фінансів Фінляндії. У лютому 2016 р. з'явився документ з електронного урядування в Фінляндії (редакція 18), де було зазначено, що основним напрямом програми реалізації кібербезпеки на державному рівні країни є подальший розвиток:

– центру з кібербезпеки;

– центрального урядового оперативного органу з інформаційної безпеки з режимом роботи 24/7;

– мережі безпеки для управління та обміном зашифрованими даними [3].

Отже, уряду Фінляндії залишається вирішити наступні нагальні питання:

– розширити можливості поліції реагувати на кіберзлочини;

– розвиток співпраці органів влади з іншими державними суб'єктами задля ефективної реалізації механізмів національної кібербезпеки;

– бути активним членом міжнародних організацій та форумів в сфері інформаційної безпеки;

– закріпити на законодавчому рівні передумови для здійснення ефективної роботи в сфері кібербезпеки;

– розробити стандарти для управління інформаційною безпекою;

– покращити рівень надання знань фахівців з питань кібербезпеки шляхом проведення наукових досліджень тощо [20].

РОЗДІЛ 3. РОЗВИТОК ЕЛЕКТРОННОГО УРЯДУВАННЯ ТА БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

3.1. Огляд стану впровадження електронного урядування в Україні

Схвалена розпорядженням Кабінету Міністрів України «Концепція розвитку електронного урядування в Україні» від 20 вересня 2017 року № 649-р визначає електронне урядування як один з інструментів розвитку інформаційного суспільства. Відповідно до даної концепції, запровадження систем е-урядування означає, що діяльність органів державної влади та органів місцевого урядування буде організована у новітніх формах, що дасть змогу сформувати новий тип держави, що задовольняє потреби громадян. За даними Державного бюджету України станом на 2020 рік, на впровадження електронного урядування було виділено близько 23 млн. грн.

Електронне урядування є дієвим засобом для взаємодії між громадянами та державою, що дає змогу вирішувати важливі запитання між органами державної влади на національному та регіональному рівнях. Організація Об'єднаних Націй з 2001 року проводить аналіз тенденцій розвитку електронного урядування у світі. ООН вимірює наскільки діяльність електронного уряду є ефективним та визначає, які інструменти впровадження є найбільш дієвими. Задля оцінки рівня розвитку ООН було створено «Індекс розвитку електронного уряду (EGDI)» та «Індекс електронної участі (EPI)» [44].

EGDI (E-Government Development Index) є одним з головних індексів розвитку електронного уряду. Він розраховується як середнє арифметичне 3-х індексів (OSI, TII, HCI):

1. Online Servise Index (широта та якість онлайн послуг) формується зі складових:

- нові інформаційні послуги (Emerging formation services);
- розширені інформаційні послуги (Enhanced information services);
- транзакційні послуги (Transactional services);

– підключені послуги (Connected services);

2. Telecommunication Infrastructure Index (Рівень розвитку комунікаційної інфраструктури) формується зі складових:

– підписки на фіксовану широкосмугову мережу (Fixed (wired) – broadband subscriptions);

– люди, які користуються Інтернетом (Individuals using the Internet);

– мобільні підписки (Mobile-cellular subscriptions);

– підписки на телефон стаціонарної мережі (Fixed-telephone subscriptions);

– підписки на бездротову широкосмугову мережу (Wireless broadband subscriptions);

3. Human Capital Index (індекс людського капіталу) формується зі складових:

– грамотність серед дорослого населення (Adult Literacy);

– показник зарахованих (Gross Enrolment Ratio);

– очікувана тривалість навчання (Expected Yearsof Schooling);

– середня кількість років навчання (Mean Years of Schooling);

4. EPI - E-Participation Index – це показник взаємодії держави з громадянами за допомогою сервісів комунікації [36].

Показники дають чітку картину розвитку країн в електронному урядуванні. Використовуючи ці дані, ми можемо проаналізувати стан е-урядування в Україні та інших країнах світу.

Проаналізуючи дані з таблиці 3.1, можна сказати, що Україна значно відстає від країн-сусідів за показником широти та якості надання онлайн-послуг. Так, у період з 2014 р. по 2020 р. Україна доклала величезних зусиль. Навесні 2015 року було впроваджено перші онлайн-сервіси в урядових структурах. Цей крок засвідчив про перехід Верховної Ради України на електронний документообіг. Зокрема, було розроблено додаток «ДІЯ», що надає користувачам широкий спектр можливостей.

Таблиця 3.1

Online Service Index (Широта та якість онлайн-послуг)

Країна	2003	2010	2014	2020
Україна	0,3493	0,3460	0,2677	0,5694
Польща	0,5415	0,3873	0,5433	0,9306
Білорусь	0,1223	0,3016	0,3228	0,7361
Румунія	0,4192	0,4159	0,4409	0,6597
Молдова	0,0699	0,2952	0,5275	0,7708
Словаччина	0,3799	0,3460	0,4882	0,7361
Угорщина	0,3122	0,5048	0,5591	0,7361
Світовий лідер	1,0000 (США)	1,0000 (Південна Корея)	1,0000 (Франція)	1,0000 (Данія)
Європейський лідер	0,7773 (Великобританія)	0,7746 (Великобританія)	1,0000 (Франція)	1,0000 (Данія)

Подальший розвиток технологій дозволив в Україні втілити концепцію «сервісної держави в національних ініціативах». Це означає, що держава активно використовує ІКТ для зв'язку з громадянами та бізнесом як споживачами її послуг. Громадяни та бізнеси тепер мають можливість отримати такі послуги, як: освіта, медичне обслуговування та соціальне забезпечення, сплатити податки, отримати ліцензії, державні закупівлі, здійснити міжнародні торгові операції, і найголовніше – розвиток електронної демократії в майбутньому [42].

Таблиця 3.2

Telecommunication Infrastructure Index (Рівень розвитку комунікаційної інфраструктури)

Країна	2003	2010	2014	2020
Україна	0,1157	0,2487	0,3802	0,4364
Польща	0,2478	0,3374	0,5618	0,5805
Білорусь	0,1472	0,2081	0,6069	0,6881
Румунія	0,1491	0,3093	0,4385	0,5471

Молдова	0,1199	0,1933	0,4235	0,4787
Словаччина	0,2941	0,4212	0,5296	0,5964
Угорщина	0,3065	0,4338	0,5654	0,6071
Світовий лідер	0,8456 (Швеція)	0,7687 (Швейцарія)	1,0000 (Монако)	1,0000 (Монако)
Європейський лідер	0,8456 (Швеція)	0,7687 (Швейцарія)	1,0000 (Монако)	1,0000 (Монако)

Зробивши аналіз показників за рівнем розвитку телекомунікаційної інфраструктури (таблиця 3.2), можна сказати, що Білорусь є лідером в цьому напрямку. Фактично кожна мережа кабельного телебачення вже перейшла до HD-формату. Зокрема, в країні активно впроваджуються IMS-платформи, а 97,1 % територій охвачує 3G зв`язок, де проживає 99,9 % країни, вже проведена робота для впровадження технологій LTE (4G) [35].

Рівень певного людського капіталу (таблиця 3.3) в Україні значно знизився, причиною цьому стала міграція населення в країни Європи.

Таблиця 3.3

Human Capital Index (Людський капітал)

Країна	**2003**	**2010**	**2014**	**2020**
Україна	0,9200	0,9647	0,8616	0,8436
Польща	0,9400	0,9552	0,8396	0,8668
Білорусь	0,9200	0,9659	0,8861	0,8681
Румунія	0,8800	0,9226	0,8100	0,7944
Молдова	0,9000	0,8999	0,7201	0,7274
Словаччина	0,9100	0,9310	0,8265	0,8141
Угорщина	0,9300	0,9597	0,8668	0,8364
Світовий лідер	1,4220 (Мікронезія)	0,9987 (Куба)	1,0000 (Нова Зеландія)	1,0000 (Австралія)

Європейський лідер	0,9900 (Бельгія)	0,9933 (Данія)	0,9619 (Ірландія)	0,9740 (Бельгія)

Треба додати, що була укладена багатостороння рамкова угода, що стосується радіочастотного плану майбутнього цифрового наземного телебачення між адміністраціями зв'язку Албанії, Австрії, Боснії і Герцеговини, Болгарії, Хорватії, Греції, Республіки Македонії, Угорщини, Чорногорії, Румунії, Сербії, Словенії, Туреччини і України.

Також активно розвивається електронна участь громадян та держави на регіональному рівні. Лідерами є: Вінниця, Львів, Київ, Дніпро, Луцьк, Харків.

До прикладу розглянемо Картку львів'янина – це персоналізована електронна картка, за допомогою якої жителі міста можуть користуватись швидше та зручніше. Дані картки є важливим елементом впровадження електронного урядування на місцевому рівні, тому з'являються і в інших містах України.

Наявність карки відкриває її власникам можливості здійснювати запит на надання адміністративних послуг, а в Особистому кабінеті мешканця (на Інтернет-порталі egov.city-adm.lviv.ua) отримати доступ до онлайн-сервісів. Кожен користувач може отримати наступні послуги:

– подати електронний запит до виконавчих органів Львівської міської ради;

– стати в чергу на прийом до державного службовця;

– зробити запит на отримання довідки про несудимість (МВС) або довідки про доходи (ДФС).

До того ж, Картка львів'янина значно спрощує процедуру отримання соціальної допомоги для учасників АТО. Так, їм не потрібно надавати паспорт, ідентифікаційний номер, довідку про склад сім'ї (Ф-2), посвідчення учасника АТО, довідку про доходи членів сім'ї (ДФС), відомості про заборгованість за комунальні послуги. Щоб отримати соціальні пільги за спрощеною процедурою необхідно звернутись до Центру надання адміністративних послуг (ЦНАП) м. Львова або до «Єдиної приймальні» Управління соціального захисту Львівської міської ради [33].

Як можна побачити (таблиця 3.4), Україна посіла 75 місце за Індексом електронної взаємодії держави та громадян станом на 2020 рік. Країни-сусіди значно випереджають Україну. Так, Молдова та Білорусь завдяки проведенні низки реформ на нормативно-правовому рівні та залученню професіоналів у даній галузи зробили великий крок уперед [25].

Таблиця 3.4

E-Participation Index (електронна взяємодія між громадянами та державою)

Країна	**2003**	**2010**	**2014**	**2020**
Україна	24 (0,3966)	48(0,2171)	77 (0,4314)	75(0,6854)
Польща	24 (0,3966)	51 (0,2429)	65 (0,4902)	31 (0,8933)
Білорусь	102 (0,0345)	51 (0,2429)	92 (0,3529)	33 (0,8820)
Румунія	91 (0,0517)	64 (0,1857)	71 (0,4706)	69 (0,7079
Молдова	102 (0,0345)	58 (0,2000)	40 (0,6275)	37 (0,8596)
Словаччина	53 (0,1724)	117 (0,0714)	40 (0,6275)	50 (0,8090)
Угорщина	37 (0,2931)	36 (0,3143)	75 (0,4510)	69 (0,7079)
Світовий лідер	1,0000 (Великобританія)	1,0000 (Південна Корея)	1,0000 (Нідерланди)	1,0000 (Данія)
Європейський лідер	1,0000 (Великобританія)	0,8286 (Іспанія)	1,0000 (Нідерланди)	1,0000 (Данія)

За індексом розвитку електронного урядування, станом на 2020 рік, Україна посіла 82 місце (таблиця 3.5).

Таблиця 3.5

E-Government Development Index (Розвиток електронного урядування)

Країна	**2003**	**2010**	**2014**	**2020**
Україна	54 (0,4617)	54 (0,5181)	87 (0,5032)	82 (0,6265)
Польща	32 (0,5764)	45 (0,5582)	42 (0,6482)	33 (0,7926)
Білорусь	81 (0,3965)	64 (0,4900)	55 (0,6053)	38 (0,7641)
Румунія	50 (0,4828)	47 (0,5479)	64 (0,5632)	67 (0,6671)

Молдова	95 (0,3633)	80 (0,4611)	66 (0,5571)	69 (0,6590)
Словаччина	40 (0,5280)	43 (0,5639)	51 (0,6148)	49 (0,7155)
Угорщина	44 (0,5163)	27 (0,6315)	39 (0,6637)	45 (0,7265)
Світовий лідер	0,9261 (США)	0,8785 (Південна Корея)	0,9462 (Південна Корея)	0,9195 (Данія)
Європейський лідер	0,8397 (Швеція)	0,8147 (Великобританія)	0,8938 (Франція)	0,9195 (Данія)

Для того, аби держава могла швидко перейти до інформаційного суспільства, науковці наголошують, що вкрай важливо розробити програму переходу. Дана програма включає в себе чітко сформовану стратегію та прописаний план дій влади для успішної реалізації інформаційної політики, насамперед:

– створення єдиного інформаційного простору держави та його інтеграція у внутрішнє і зовнішнє середовище;

– створення та вдосконалення інформаційної інфраструктури держави;

– розробка інформаційних продуктів і надання послуг;

– інформаційні ресурси повинні включати різні сфери та бути присутніми на різних рівнях;

– розвиток засобів масової інформації;

– розвиток нових форм підприємництва, освіти, науки, соціальної сфери з використанням новітній інформаційних технологій;

– забезпечити захищеність інтелектуальної власності в інформаційному просторі;

– створити систему регулювання і контролю над використанням інформаційних технологій. Забезпечити суспільство та державу від дезінформації [34].

Проаналізувавши стан розвитку електронного урядування в Україні можна дати наступні рекомендації: проводити комунікацію з громадянами:

– проводити комунікацію з громадянами: інформувати про впровадження нових сервісів, їх функціонал та як можна отримати ці послуги;

– мотивувати та залучати молодих, креативних та сучасних ІТ-спеціалістів нашої країни до роботи;

– використовувати досвід провідних країн світу, що успішно впровадили е-урядування, для покращення взаємодії громадян та держави.

Для вдосконалення телекомунікаційної інфраструктури вже зроблені, вагомі кроки, в недалекому майбутньому це дасть своє позитивне зрушення з місця, попри це, необхідно покращити зв`язок 3G та 4G у сільських та гірських регіонах, покращити рівень широкосмугового доступу та посилити співпрацю з сусідніми країнами для здобутку взаємовигідних цілей на просторі телекомунікації інфраструктури. Крок за кроком українській владі вдається успішно впровадити е-урядування, але необхідно допрацювати зроблені кроки в усіх складових E-Government Development Index (індекс електронного урядування).

На шляху впровадження е-урядування наша держава стикається з наступними проблемами, а саме:

– низький рівень довіри громадян;
– низький рівень обізнаності населення в електронних сервісах;
– слабкий рівень захищеності електронних ресурсів від кібератак;
– халатність та низький рівень кваліфікації працівників;
– недостатнє фінансування та брак технічних ресурсів;
– низький рівень комунікації державних сайтів з громадянами [36].

Необхідно залучати найкращих спеціалістів країни на державну службу, для нових спеціалістів потрібні радники з успішних країн по електронному врядуванню. Існує проблема незахищеності електронних ресурсів від хакерських атак. Хоча у жовтні 2015 р. був заснований Департамент кіберполіції Національної поліції України, який в березні запустив кампанію з обізнаності громадян про кібербезпеку.

Для того аби підвищити рівень обізнаності населення потрібно налагодити інформування на національних, місцевих каналах та використовувати соціальні

мережі, як один з інструментів комунікації з громадськістю. Веб-сайти міністерств та веб-сайти регіонального рівня, іноді несвоєчасно публікують інформацію, закони, акти, тощо. Ще одним з недоліків сайті є неструктурованість інформації, через що складно знайти те, що потрібно.

Отже, впровадження електронного урядування в Україні, у порівнянні з іншими державами, відбувається дещо складніше. Стрімкому розвитку е-урядування стоїть на заваді низка проблем, таких як, низький рівень довіри громадян, недостатнє фінансування, недостатня кількість професіоналів тощо. З кожним роком росте кількість країн, де передбачене онлайн обслуговування для вразливих верств населення.

Більшість країн стали дотримуватися підходу «спочатку в цифрі» при запроваджені е-уряду. Проте не всі громадяни можуть користуватись послугами, адже хтось може не вміти користуватись Інтернетом. Для того, аби охопити усе населення, незалежно від місця їх проживання або їх можливостей електронного включення, важливо розвивати сферу державного обслуговування, як онлайн так і офлайн [17].

Незважаючи на те, що держава робить вагомі кроки у напрямку розвитку є необхідність залучати висококваліфікованих вітчизняних фахівців на державну службу, проводити підвищення кваліфікації та навчання новим технологіям та протоколам роботи державних службовців. А також активна співпраця з країнами, які мають успіхи в запровадженні систем е-урядування.

Отже, розвиток е-урядування повинен відбуватись в різних площинах (індустріального, організаційного та технічного забезпечення). Спільна робота державного сектора, бізнес структур та приватно-публічного партнерства відіграють важливу роль у створенні «цифрового суспільства». Це дозволить залучити громадян до політики, процедури прийняття рішень, розробки та надання послуг за допомогою використанні інформаційно-комунікаційних технологій.

3.2. Політико-правові норми захисту даних систем електронного урядування в Україні

Концептуальні засади державної політики у сфері інформатизації, розвитку інформаційного суспільства та електронного урядування визначено насамперед у низці законодавчих актів, таких як: Закон України «Про інформацію» від 02.10.1992 № 2657-XII, Закон України «Про науково-технічну інформацію» від 25.06.1993 № 3322-XII, Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 № 537-V, Закон України «Про Національну програму інформатизації» від 04.02.1998 №74/98-ВР, Закон України «Про Концепцію Національної програми інформатизації» від 04.02.1998 №75/98-ВР, Закон України «Про телекомунікації» від 18.11.2003 № 1280-IV, Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI, Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР, Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV, Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII та інші.

Згідно з цими та низкою інших актів інформаційного законодавства держава визначається, як головний організуючий, координуючий та контролюючий орган у відносинах між її суб'єктами: держава – бізнес, держава – громадяни, держава – міжнародні/громадські організації. Саме тому перераховані вище документи вказують на приналежність до інформаційного законодавства положень, статей з нормативно-правових актів адміністративного законодавства. А в адміністративному законодавстві, навпаки, містяться інформаційно-правові норми [9].

Адміністративне законодавство є зовнішньою формою вираження адміністративно-правового регулювання та займає вагоме місце в системі нормативно-правового регулювання електронного урядування.

Проаналізувавши нормативно-правові акти, можна чітко сказати, що система нормативно-правового регулювання е-урядування в органах виконавчої влади

України вимагає вдосконалення, шляхом проведення реформування у правовому полі. Ретельного перегляду норм вимагає адміністративне законодавство.

Системи електронного урядування в адміністративному законодавстві регулюють такі нормативні акти: Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 № 3475-IV; Закон України «Про звернення громадян» від 02.10.1996 № 393/96-ВР [2], а також Закон України «Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції» від 02.07.2015 № 577-VIII, в якому було внесено зміни, що значно розширюють можливості реалізації прав громадян на звернення до органів державної влади та місцевого самоврядування за допомогою сучасних засобів, наприклад: петиції або електронні звернення; Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI [3] та Закон України «Про внесення змін до деяких законів України щодо доступу до публічної інформації у формі відкритих даних» від 09.04.2015 № 319-VIII, де було зазначено про зміну форми відкритих даних, аби доступ до них був відкритим.

Основна мета Закону від 09.04.2015 № 319-VIII полягає в забезпеченні реалізації права особи на вільний доступ до інформації, що містить суспільні інтереси, а також відкритість діяльності органів державної влади місцевого самоврядування. Дані цілі можна досягти шляхом впровадження механізмів оприлюднення інформації у вигляді відкритих даних. Відповідно до положень Закону розпорядники інформації повинні надавати публічну інформацію на державному веб-порталі та веб-сайтах, як відкриті дані на запит, а також публікувати та оновлювати її на регулярній основі.

Крім того, не можна не згадати про такий важливий закон, як Закон України «Про адміністративні послуги» від 06.09.2012 № 5203-VI, в якому визначено «…правові засади реалізації прав, свобод і законних інтересів фізичних та юридичних осіб у сфері надання адміністративних послуг». Законом України «Про внесення змін до деяких законодавчих актів України щодо розширення повноважень органів місцевого самоврядування та оптимізації надання адміністративних послуг» від 10.12.2015 № 888-VIII до Закону України «Про адміністративні послуги» та інших

законів були внесені, на наш погляд, кардинальні зміни. Тепер стало можливим подавати заяви на отримання адміністративних послуг в режимі онлайн [16].

Єдиний державний портал адміністративних послуг та інші інтегровані в нього системи є тими сервісами, що надають адміністративні послуги користувачам.

До того ж, питання розвитку інформаційного суспільства та інформаційної сфери в цілому, впровадження електронного урядування регулюються низкою підзаконних нормативних актів, зокрема, актами Верховної Ради України (далі – ВРУ) («Постанова ВРУ «Про затвердження Завдань Національної програми інформатизації на 2006–2008 роки» від 04.11.2015 № 3075-IV; «Постанова ВРУ «Про Рекомендації парламентських слухань на тему: «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України» від 31.03.2016 № 1073-VIII, тощо); актами Кабінету Міністрів України (далі – КМУ), а саме: постановами КМУ («Постанова КМУ «Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів» від 17.03.2004 № 326; «Постанова КМУ «Про запровадження Національної системи індикаторів розвитку інформаційного суспільства» від 28.11.2012 № 1134; «Постанова КМУ «Про затвердження Положення про формування та виконання Національної програми інформатизації» від 31.08.1998 № 1352; «Постанова КМУ «Про заходи щодо створення електронної інформаційної системи «Електронний Уряд» від 24.02.2003 № 208; «Постанова КМУ «Деякі питання оприлюднення публічної інформації у формі відкритих даних» від 30.11.2016 № 867; тощо) та розпорядженнями КМУ («Розпорядження КМУ «Про затвердження Концепції формування системи національних електронних інформаційних ресурсів» від 05.05.2003 № 259-р; «Розпорядження КМУ «Про затвердження заходів з реалізації Концепції формування системи національних електронних інформаційних ресурсів» від 31.12.2003 № 828-р; «Розпорядження КМУ «Про затвердження плану заходів з виконання завдань, передбачених Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 15.08.2007 № 653-р.; «Розпорядження КМУ «Питання реалізації пілотного проекту впровадження технологій електронного урядування» від 01.03.2010 № 360-р; «Розпорядження КМУ «Про схвалення Стратегії

розвитку інформаційного суспільства в Україні» від 15.05.2013 № 386-р; «Розпорядження КМУ «Про схвалення Концепції розвитку електронного урядування в Україні» від 13.12.2010 № 2250; «Розпорядження КМУ «Про затвердження плану заходів щодо реалізації Концепції розвитку електронного урядування в Україні» від 26.09.2011 № 1014; «Розпорядження КМУ «Про схвалення Концепції розвитку електронного урядування в Україні» від 20.09.2017 № 649-р; «Розпорядження КМУ «Про затвердження плану заходів з реалізації Концепції розвитку електронного урядування в Україні» від 22.08.2018 № 617-р; «Розпорядження КМУ «Про затвердження плану заходів щодо реалізації Концепції розвитку системи електронних послуг в Україні на 2019 – 2020 роки» від 30.01.2019 № 37-р; тощо); актами Президента України, що видаються Президентом України у межах його повноважень, що ґрунтуються на основних засадах Конституції і законів України («Указ Президента України «Про Положення про технічний захист інформації в Україні» від 27.09.1999 № 1229/99; «Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31.07.2000 № 928/2000; «Указ Президента України «Про першочергові завдання щодо впровадження новітніх інформаційних технологій» від 20.10.2005 № 1497/2005; «Указ Президента України «Про Стратегію сталого розвитку «Україна - 2020» від 12.01.2015 № 5/2015; тощо) та іншими підзаконними нормативними актами [42].

Таким чином, впровадження електронного урядування в Україні регулюється великою кількістю нормативних актів. Причому в цих актах адміністративно-правові та інформаційно-правові норми тісно пов’язані між собою.

Однак відсутність єдиної державної політики з упровадження електронного урядування, її концептуальних засад та стратегії, відсутність чітко визначеної системи критеріїв їх реалізації, а також дієвого контролю з боку держави за виконанням заходів із впровадження електронного урядування призвели до того, що Україна значно відстає за темпами впровадження електронного урядування від інших європейських країн.

У 1998 р. було прийнято Закон України «Про Національну програму інформатизації» від 04.02.1998 № 74/98-ВР. Це стало першим кроком до впровадження механізмів та інструментів електронного. Стаття 5, зазначає, що «Головною метою Національної програми інформатизації є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави. Законом України «Про Концепцію Національної програми інформатизації» від 04.02.1998 №75/98-ВР було визначено довгострокові цілі та загальні принципи інформатизації, очікувані наслідки після їх запровадження [33].

Крім того, відповідними рішеннями Уряду, прийнятими ще у 2002-2005 рр., передбачалось: створити та інтегрувати електронні інформаційні системи та ресурси у Єдиний веб-портал органів виконавчої влади та надавати інформаційні чи інші послуги через електронну інформаційну систему «Електронний Уряд» (2004-2005 р.); створити електронну інформаційну систему «Електронний Уряд» (2004-2005 рр.); забезпечити надійний захист інформації, що доступна в Єдиному веб-порталі органів виконавчої влади та інтегрованих в нього веб-сайтів, електронних інформаційних системах і ресурсах органів виконавчої влади (2004-2005 рр.); розробити та затвердити перелік і порядок надання інформаційних та інших послуг з використанням електронної інформаційної системи «Електронний Уряд» (2003 р.) тощо.

Однак, закріплюючи низку заходів, спрямованих на впровадження електронного урядування, ці нормативно-правові акти не визначали чіткий план дій, їх взаємозв’язку, технічне та ресурсне забезпечення, очікувані результати тощо.

На превеликий жаль, Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007- 2015 рр.» від 09.01.2007 № 537-V, в якому визначено вектори розвитку інформаційного суспільства в Україні та впровадження новітніх ІКТ як в діяльність державних органів, так і в життя населення, та схвалена розпорядженням КМУ від 13.12.2010 № 2250-р Концепція

розвитку електронного урядування в Україні, що була спрямована на розвиток електронного урядування, мають більш загальний, декларативний характер [25].

Так як план заходів щодо реалізації цієї Концепції розвитку електронного урядування, затверджений Розпорядженням КМУ від 26.09.2011 р. №1014-р не було виконано, КМУ на своєму засіданні 20 вересня 2017 р. затвердив нову «Концепцію розвитку електронного урядування в Україні». У Концепції було визначено головні цілі, пріоритети та дії направлені на розвиток.

До того ж, є проблема низького рівню підготовки до складання нормативно-правових актів. У більшості випадків на етапі підготовки до розробки актів не відбувається ретельний аналіз проблеми, що потребує правового регулювання, а можливі ризики після їх впровадження не враховуються. Окрім цього бракує якісної соціально-економічної та правової експертизи, громадської дискусії тощо. Отже, можна сказати, що в Україні відсутній цілісний механізм правового забезпечення виконання завдань, що стосуються впровадження е-урядування. Ще одною проблемою є брак досвіду правозастосування та зневажливе ставлення до правових принципів громадян та бізнесу, навіть державних службовців.

Програма діяльності Кабінету Міністрів України визначає основні довгострокові пріоритети для діяльності Уряду. Основні положення даного документу визначають: довгострокове планування, короткострокове планування для визначення плану дій по вдосконаленню вузьких сфер, програми для реалізації проектів, які фінансуються державою [32].

3.3. Перспективи розвитку електронного урядування та боротьби з кіберзлочинністю в Україні

У сучасному світі відбувається чимало глобальних процесів, що змінюють наше життя. Одним з таких є створення електронних урядів та використання технологій е-урядування задля розвитку інформаційного суспільства та електронної демократії. Інформатизація процесів діяльності органів влади та управління сприяє забезпеченню прозорості та відкритості їхньої роботі, що є основоположним

принципом демократичності суспільства. Майже всі держави світу працюють над впровадженням електронних урядів, адже застосування найсучаснішого світового досвіду цифровізації урядування доволі швидко дозволяє підвищити інституційну спроможність будь-якої країни.

Задля того, аби оцінити результати впровадження електронного урядування використовуються дані світових рейтингів, які відображають стан електронного урядування в різних країнах на основі загальноприйнятих показників. Зважаючи не це, особливої уваги потребує аналіз показників розвитку електронного урядування в Україні та порівняння їх з іншими країнами світу. Даний аналіз дасть змогу знайти можливі шляхи вдосконалення надання онлайн послуг та публічної інформації органами держаної влади громадянам, телекомунікаційної інфраструктури та розвитку людського капіталу.

Електронне урядування є формою організації державного управління наряду з іншими інструментами розвитку інформаційного суспільства. Використання систем електронного урядування дасть змогу забезпечити ефективність, відкритість та прозорість діяльності органів державної влади та місцевого самоврядування. Електронне урядування вирішує ряд завдань в політичній, соціальній, технологічній та економічній сферах. Що стосується політичної сфери, то можна значно покращити внутрішні та зовнішні взаємовідносини, збільшити показник відкритості та прозорості діяльності органів влади, а також оптимізувати роботу державного адміністративного апарату використовуючи інформаційно-комунікаційні технології [15].

У соціальній сфері електронне урядування виконує наступні завдання: підвищує рівень задоволеності громадян процесом надання державних та адміністративних послуг; створює якісний сучасний ринок інтелектуальних послуг; надає поштовх до розвитку інфраструктури телекомунікацій за рахунок впровадження технологій електронного урядування в технологічній сфері. Не менш важливим є скорочення кількості урядових видатків, видатків громадян та бізнесових структур за допомогою зменшення часових витрат на надання/отримання послуг[3] .

Впровадження електронного урядування в Україні має такі позитивні зміни:

– робота органів влади стає відкритою та прозорою;

– надання адміністративних послуг надаються швидше та якісніше;

– громадяни забезпечені доступом до публічної інформації завдяки сучасним інформаційним технологіям;

– економія часових та матеріальних ресурсів урядів, громадян та бізнесу;

– державо службовці звільнені від рутинної роботи;

– підвищення рівня демократизації суспільства [4].

Підтвердити ефективність систем електронного урядування можна проаналізувавши досвід світових лідерів. У 2003 році було створено Департамент з економічних і соціальних питань ООН (UNDESA). Раз на два роки дана організація проводить оцінювання рівню розвитку електронного урядування за індексом EGDI (E-Government Development Index). Індекс EGDI є комплексним показником, що утворюється через сукупність інших індексів та використовується для вимірювання готовності національних адміністрацій до використання інформаційно-комунікаційних технологій для надання якісних інформаційних послуг населенню, бізнесу та застосування їх у роботі самих органів влади [40].

В основі Індексу розвитку електронного уряду EGDI лежить три субіндекси: OSI (Online Service Index) – онлайн-сервіси, розраховується «Департаментом з економічних і соціальних питань ООН (UNDESA)»; «TII (Telecommunication Infrastructure Index)» – телекомунікаційна інфраструктура, розраховується Міжнародним союзом електрозв'язку ITU; та «HCI (Human Capital Index)» – людський капітал, розраховується ЮНЕСКО спільно з «Програма розвитку ООН» [5].

Покращення показників розвитку електронного уряду та електронної участі в Україні вдалось досягти шляхом впровадження наступних механізмів е-урядування [10]:

– застосування нових інструментів е-урядування підвищують ефективність та прозорість роботи органів влади, а також надають електронні послуги втричі більше в 2018 р. порівняно з попереднім;

– покращена процедура електронного документообігу в органах влади, що дало змогу підключити до систем електронної взаємодії органів виконавчої влади 193 органи влади, установи та організації протягом 2018 р.; на сьогодні електронна міжвідомча взаємодія впроваджена у 673 органах влади;

– відбувається активний розвиток сфери відкритих даних; так у 2020 р. Україна посіла 17 сходинку в світі у сфері відкритих даних, та друге місце – за темпами розвитку за останні чотири роки;

– здійснення державних та комерційних закупівель в Україні через систему публічних закупівель ProZorro та відкриту систему комерційних закупівель RIALTO, що надає публічний доступ до усіх закупівель, дозволяє взяти участь у закупівлях, запропонувати державі та бізнесу товари або послуги та скористатися всіма супутніми сервісами;

– розвиток інструментів е-демократії на місцевому рівні (понад 130 громад уже запровадили е-петиції, якими користується уже понад 1 мільйон українців). На національному рівні розвиток електронної демократії відбувається повільніше. Для того, аби прискорити цей процес варто розробити та дотримуватись «Концепції розвитку електронної демократії»;

– створення е-платформ в сфері освіти («Національна електронна платформа», «Нова українська школа», е-платформа «Everest» та ін.), що надають безкоштовний доступ до навчальних матеріалів в електронному вигляді, в обсязі та за предметами, передбаченими навчальною програмою. Це також сприяє розвитку ринку виробництва електронних освітніх продуктів та сервісів, а також поширенню електронного навчання та формуванню цифрової компетентності учасників освітнього процесу в Україні;

– активне використання та удосконалення інклюзивних платформ з обговорення та формування політики в сфері електронного урядування та електронної демократії в кожному з регіонів країни;

– можливість регіонів відстоювати свої потреби, ідеї та інтереси щодо впровадження електронного урядування та електронної демократії на загальнодержавному рівні.

Подальше використання механізмів електронного урядування для підзвітності та прозорості влади в Україні залишається перспективним, це обумовлено наступними факторами [8]:

– подальше покращення якості послуг та доступність до публічної інформації для громадян, можливе лише завдяки формуванню та впровадженню загальноприйнятих стандартів електронного урядування;

– застосування владою новітні інформаційно-комунікаційні технології підвищує прозорість та відкритість органів влади;

– роль організацій громадянського суспільства у адвокації, мобілізації та просуванні е-демократії збільшується. Що забезпечить більш активну участь громадян у процесі прийняття рішень на місцевому та регіональному рівнях в майбутньому;

– безперервне покращення систем електронного урядування та демократії з урахуванням потреб регіонів України;

– сприяння інклюзивному діалогу стосовно створення політики е-урядування та е-демократії, що ґрунтується на інтересах та потребах регіонів;

– довіра громадян до інститутів публічної влади підвищується;

– зниження рівню корупції в Україні.

Станом на сьогодні, цифрові технології повинні бути першим пріоритетом з огляду на світові тенденції розвитку електронного урядування. Використання даних технологій зможе забезпечити ряд переваг для співпраці в таких галузях як: електронна комерція, електронна митниця, електронна охорона здоров’я, безпаперова торгівля, електронні комунікації, мережева та інформаційна безпека, кібербезпека, електронна ідентифікація і довірчі послуги, цифрові навички та просування інновацій, відкриття даних та ін. [4].

Підсумовуючи вищезазначене, слід наголосити увагу на тому, що завдяки плідній роботі владних структур та позитивні результати у впровадженні механізмів електронного урядування в Україні за останні чотири роки значно покращили показників розвитку електронного уряду та електронної участі. За чотирьохрічний період задля успішного впровадження та розвитку електронного урядування в Україні було прийнято нормативно-законодавчу базу та сформовано відповідні організаційні передумови. Завдяки впровадженню та розвитку електронного урядування, як держава, так і суспільство, чітко зрозуміли, що це значно підвищує рівень прозорості та відкритості органів публічної влади, громадяни більше залучені до демократичних процесів. І найголовніше – це зниження рівня корупції в Україні.

McAfee – це американська компанія, що входить до складу Intel Corporation. McAfee є розробником антивірусного програмного забезпечення. У 2012 році дана компанія стала одним із спонсорів програми зі створення глобального звіту про стан світової кібербезпеки [2]. Звіт було складено брюссельською компанією Security & Defence Agenda. Аналітики центру вперше публічно висвітлили проблему можливих кібератак інформаційних систем різних країн. Основна мета звіту – показати урядам та організаціям їх рівень кібернетичної незахищеності в порівнянні з іншими країнами.

Для складання звіту було залучено групу експертів, що складалась з 80 фахівців з 27 країн світу. Результатами роботи аналітиків були висновки про поточну готовність до кібератак інформаційних систем різних країн.

Під час виконання дослідження було використано метод анонімного опитування. Респондентами виступили 250 професіоналів у галузях ІТ-технології, інформаційної безпеки, захисту інформації, боротьби з кіберзлочинністю та ін. з 21 країни. Після завершення дослідження та оформлення висновків групою експертів було проведено ранжування. Результати були подані у вигляді рейтингу по 5-бальній системі. Готовність країн (з переліку в таблиці нижче) до можливих кібератак було представлено у вигляді рейтингу – табл 3.6.

Таблиця 3.6

Стан готовності до кібератак інформаційних систем деяких країн

Рейтинг	Країна
5	–
4,5	Фінляндія, Ізраїль, Швеція
4	Данія, Естонія, Франція, Німеччина, Нідерланди, Іспанія, Великобританія, США
3,5	Австралія, Австрія, Канада, Японія
3	Китай, Італія, Польща, Росія
2,5	Бразилія, Індія, Румунія
2	Мексика

З 23-ох країн найвищі результати, а саме 4,5 бали, отримали Швеція, Ізраїль та Фінляндія. Такі світові лідери як: США, Велика Британія, Франція та Німеччина, на ряду з Данією, Естонією, Нідерландами та Іспанією посіли друге місце отримавши 4 бали. Польща, Італія, Китай та Росія зайняли 4 місце маючи 3 бали. Проаналізувавши дані звіту Security & Defence Agenda, питання чи біло виставлено бали Україні залишається відкритим.

На основі звіту можна виокремити наступні висновки експертів.

Отже, статистика демонструє наступне:

– 57% респондентів впевнені, що «гонка озброєнь» присутня і в кіберпросторі;

– 36% переконані, що кібербезпека є більш важливою та актуальною проблемою, аніж протиракетна оборона;

– 43% найбільшою загрозою з руйнівними економічними наслідками визначили створення кібернитичних перешкод або нанесення збитків життєво важливим інфраструктурам;

– 45% опитуваних відзначили, що питання кібербезпеки має бути на одному ж рівні з питанням безпеки кордонів держави;

– 56% зазначають, що висококваліфікованих фахівців з питань кібербезпеки недостатньо. І наголошують на необхідності вирішення проблеми підготовки кваліфікованих кадрів.

У звіті Security & Defence Agenda група експертів також висвітлює низку зауважень та проблем над якими варто попрацювати. Серед них основними є:

– глобальний обмін інформацією повинен здійснюватися в режимі реального часу, чого зараз бракує;

– необхідне додаткове фінансування приватному та державному секторам для покращення кібернетичної безпеки;

– правоохоронні органи по боротьбі з транскордонною кіберзлочинністю бракує повноваження для здійснення свої функцій;

– необхідно налагодити процедуру обміну досвідом кращих інститутів з міжнародної безпеки для ефективної доробки ти впровадження технологій боротьби з кіберзлочинністю;

– досягнуті кібердомовленості повинні бути чіткими та адресованими;

– мережа кампаній з інформування населення щодо засобів захисту від кібератак доволі вузько поширені, тому потрібно попрацювати над їх удосконаленням та розширенням.

Опитувані респонденти майже одностайно дійшли до висновку, що для того, щоб боротьба з кіберзлочинністю була максимально ефективною необхідно налагодити глобальний обмін інформацією в режимі реального часу. Обмін інформацією повинен бути оперативним та швидким, адже це має прямий вплив на прийняття управлінських рішень.

Такої ж думки дотримуються експерти Європейського агентства з мережевої та інформаційної безпеки (англ.: European Network and Information Security Agency – ENISA). ENISA у своїй «Програмі надійності та захисту ключової інформаційної інфраструктури» (англ.: Cisco International Internship Program – CIIP) настоює на тому, що вкрай важливо налагодити співпрацю задля того, аби гарантувати узгодженість характерних методів та засобів боротьби з кіберзлочинністю [2].

На сьогоднішній день більшість країн світу вже мають налагоджену систему співробітництва та визначену необхідність в обміні досвідом на міжнародному рівні. У кожній країні є свою розроблена та діюча стратегія кібербезпеки, що і координує дане питання. Наприклад, в стратегіях США та більшості країн Європейського Союзу питанням боротьби з кібератаками та злочинністю приділено особливу увагу.

Що стосується досвіду України, то стратегія захисту кіберпростору знаходиться в стані розробки. Тому, обмін досвідом та інформацією з країнами, які вже тривалий час працюють над забезпеченням безпеки та удосконаленням засобів захисту, є надзвичайною цінністю для держави. Незважаючи на те, що положення стратегії кожної держави можуть бути різними з огляду на політичні та технічні фактори, основні принципи залишаються незмінними.

Проаналізувавши стратегії кібербезпеки деяких країн світу [2], можна виокремити наступні загальноприйняті фактори:

– урядова модель повинна бути спрямована на захист кіберпростору від атак та іншої злочинності;

– повинен бути чітко визначений механізм суспільно-державного партнерства, що забезпечить приватних та державних осіб можливістю вести діалог та затверджувати рішення, що стосуються проблеми кібербезпеки;

– як у приватному, так і в державному секторах повинні бути затвердженні політики та регулюючі механізми, чітко визначені ролі, права та відповідальності у галузі захисту від кіберзлочинності;

– прийняття участі у міжнародній боротьбі з кіберзлочинністю для набуття досвіду та подальшого його використання для розвитку можливостей держави;

– інформаційні структури, що відповідальні за захист повинні бути чітко визначеними;

– повинен бути затверджений план дії у разі здійснення атак або збоїв та налагоджена роботи задля своєчасної реакції на такі випадки;

– для державного управління ризиками потрібно розробити системний та інтегрований підхід;

– цілі інформаційних програм повинні бути визначеними як пріоритетні та покликані до покращення взаємодії користувачів з владою;

– навчання нових фахівців з питань кібербезпеки та підвищення кваліфікації вже існуючим має бути акцентом у нових освітніх програмах;

– посилення важливості та розвиток міжнародної співпраці.

Питання боротьби з кіберзлочинністю в нашій країні є дуже актуальним. У [3], присвяченій динаміці злочинів у сфері високих технологій в банківській системі, містяться дані про існування стійкої тенденції до збільшення кількості кіберзлочинів в Україні. При цьому, протягом останніх років кількість розкритих злочинів у сфері ІТ-технологій в Україні майже не змінилося, хоча в сфері комп'ютерних та Інтернет-технологій, кількість розкритих злочинів збільшилося в кілька разів. Враховуючи вищезазначене, рівень захищеності інформації в Україні свідчить про необхідність підтримки, вдосконалення та розвитку.

Отже, з активним розвитком технологій та мережі Інтернет середовище кіберпростору стає дедалі вразливішим до можливих загроз. Саме тому методи боротьби та засоби захисту від кіберзлочинів потребують безперервного вдосконалення. А влада, у той самий час, повинна будувати міцну модель, що зможе забезпечити захист свого кіберпростору.

ВИСНОВКИ

З моменту становлення інформації, як основного чинника світового розвитку, з'явилися і супутні даному явищу загрози, а там, де є загрози, є і феномен безпеки. Таким чином, перебіг людського розвитку сам собою закріпив за поняттям кібербезпеки характеристику невід'ємного елемента суспільного буття. Як було з'ясовано, на етапі феномен став означати щось більше, ніж процес захисту інформації та ресурсів її зберігання. Вирішальне значення у питанні його сприйняття стали відігравати зовнішні і внутрішні суб'єкти кіберсередовища, що безперервно впливають на формування явища як такого. Одним з основних факторів впливу на феномен кібербезпеки, що розглядається, стало навколишнє його нормативно-правове поле, фактично створює образ і характерні риси явища. Однак, чи здатне це поле ефективно впливати на кіберсередовище і на феномен кібербезпеки, зокрема? І як людству може бути підвладний контроль за невловимим кібернетичним простором, якщо часто воно не може керувати навіть видимими речами? Подібна дилема стала основною мотивацією до проведення глибшого вивчення правових аспектів забезпечення кібербезпеки.

Першим етапом на шляху вирішення дилеми, що склалася, став аналіз сутності кіберпростору і відображення його сприйняття в різних куточках планети. Історична ретроспектива дозволила виділити процес еволюції феномена Інтернету, що став основою для формування кібернетичного простору, а також частково обґрунтувати позиції деяких сторін щодо оцінки явища кібербезпеки. Загалом, виходячи з сукупності поглядів світової спільноти, кібербезпека визначається комплексом реалізованих заходів, що вживаються як на державному, так і на міжнародному рівнях з метою досягнення стабільності та захищеності кібернетичного простору та інформації, що переміщується в ньому, а також розвитку прогресивних механізмів протидії загрозам у кіберпросторі.

Визначення протидії загрозам безпеки в інформаційних системах становить комплексну проблему, для вирішення якої необхідно поєднання заходів на

законодавчому, адміністративному, процедурному і програмно-технічного рівнів інформаційної безпеки (ІБ).

Розробка та прийняття нормативно-правових актів у галузі захисту інформації покликані врегулювати безпечне використання інформаційно-комунікаційних технологій, доступу до інформації, захисту інформації від несанкціонованого доступу та витоку технічними каналами.

Призначення адміністративного рівня протидії загрозам інформаційної безпеки має зводитися до таких важливих практичних кроків як визначення керівних документів і стандартів, підходів до управління ризиками та сертифікація на відповідність стандартам інформаційної безпеки.

До процедурного рівня протидії загрозам відносяться організаційні заходи інформаційної безпеки. Важливою частиною побудови процедурного та програмно-технічного рівнів протидії загрозам інформаційної безпеки в системах е-урядування є розробка політики безпеки.

Політика безпеки (ПБ) в організаціях, підключених до систем е-урядування, являє собою сукупність принципів, правил, процедур і практичних рішень у галузі ІБ, які регулюють керування, захист та розподіл інформації, що захищається. ПБ залежить від багатьох чинників.

ПБ повинна враховувати сучасний стан та найближчі перспективи розвитку інформаційних технологій, мету, завдання, правові основи експлуатації ІС, режими функціонування об’єктів, містити аналіз загроз безпеки та способи їх реалізації.

Програмно-технічний рівень протидії загрозам ІБ передбачає такі механізми безпеки як ідентифікація і аутентифікація користувачів, управління доступом до ІС, протоколювання і аудит; криптографію, екранування каналів зв’язку, забезпечення високої доступності і т.п.

Всі розглянуті світові моделі впровадження електронного урядування є обумовленими розвитком інформаційно-комунікативних технологій і орієнтовані на майбутнє. Умовами їх реалізації виступає мережева організація суспільства, ефективно налагоджений зворотний зв'язок і високий технологічний рівень оснащеності публічного апарату.

Впровадження технологій електронного урядування вирішує ряд політичних проблем, таких як підвищення рівня прозорості надання публічних послуг, збільшення ефективність публічного управління, запобігання корупції, а також відкриває нові канали для комунікації між владою і суспільством, що є актуальними проблемами для України.

З урахуванням того, що значна кількість розвинених країн почали процес впровадження електронного урядування задовго до розробки подібних заходів в Україні, застосування успішних практик зарубіжних країн стає необхідним фактором досягнення цілей електронного урядування, попередження можливих проблем інформатизації органів влади і розвитку інформаційного суспільства.

Разом з тим, при використанні досвіду впровадження електронного урядування інших країн необхідно виділяти не лише світові тенденції, закономірності, принципи, підходи, методи створення та впровадження електронного урядування, але розуміти особливості тієї чи іншої країни, її пріоритети, специфіку розвитку, ресурсні можливості тощо. Це потребує детального дослідження кожної країни і в жодному разі не може бути просто скопійовано для використання в Україні.

СПИСОК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Волошин Ю. О. Проблема міждисциплінарності у визначенні категорії «інтеграція» та її роль у розвитку національного конституційного права. Вісник Інституту Верховної Ради України. 2011. №4. С. 16-23.
2. Голобуцький О. П. Електронний уряд / О. П. Голобуцький, О. Б. Шевчук. – К. Атлант UMS, 2002. 173 с.
3. Грицяк Н. В. Державна політика у сфері надання доступу до публічної інформації : навч.-метод. матеріали. Київ: НАДУ, 2016.32 с.
4. Грицяк Н. В. Державне управління в умовах розвитку інформаційного суспільства : навч. посіб. Київ : К.І.С., 2015. 108 с.
5. Грицяк Н. В., Соловйов С. Г. Електронна демократія : навч. посіб. Київ : НАДУ, 2015. 66 с.
6. Грицяк Н.В. Електронна демократія як механізм політичної взаємодії : наук.-метод. розробка Київ : НАДУ, 2013. 44 с.
7. Джоан К. Р., Крістіан В. А. Електронна демократія : сподівання та проблеми. Київ : Центр адаптації державної служби до стандартів Європейського Союзу, 2009. 126 с.
8. Дзюба С.В., Жиляєв І.Б. Електронне урядування : опор. конспект лекцій. – Київ : [б.в.], 2012. 67 с.
9. Дніпренко Н. К. Електронна демократія. Вітчизняний і зарубіжний досвід впровадження електронного урядування : зб. матеріалів наук.-практ. конф. К.: НАДУ, 2018. С. 85-88.
10. Дубов Д. В. Основи електронного урядування : навч. посіб. / Д. В. Дубов, С. В. Дубова. К. : Центр навчальної літератури, 2006. 176.
11. Електронне урядування : підручник / авт. кол. : В. П. Горбулін, Н. В. Грицяк, А. І. Семенченко, О. В. Карпенко та ін. ; за заг. ред. проф. Ю. В. Ковбасюка ; наук. ред. проф. Н. В. Грицяк, проф. А. І. Семен- ченка. К. : НАДУ, 2014. 352 с.
12. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – Київ, 2017. Частина 4: Публічна політика

та управління розвитком інформаційного суспільства та електронного урядування / [А.І. Семенченко, А.О. Серенок]. Київ : ФОП Москаленко О. М., 2017. С. 7-15

13. Єганов В. В. Проблеми та перспективи впровадження системи електронного урядування в Україні [Електронний ресурс]. URL: http://www.kbuapa.kharkov.ua/e-book/db/2012-2//1/05.pdf (дата звернення 17.03.2022).

14. Інформаційна та кібербезпека: соціотехнічний аспект / Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Київ : за заг. ред. док. техн. наук, професора Толубка В. Б. Київ : ДУТ, 2015. 288 с.

15. Камінська Т., Камінський А., Пасічник М. Зарубіжний досвід упровадження електронного урядування. Київ, 2008. 200 с.

16. Капніна Л. В. Аналіз динаміки розвитку електронного урядування в Україні. Математичні методи, моделі та інформаційні технології в управлінні підприємством : зб. наук. праць III студ. наук. конф. (м. Вінниця, 5 листопада 2018 р.). Вінниця : ВТЕІ КНТЕУ, 2018. С. 144–117.

17. Капніна Л.В., Ніколіна І.І. Оцінювання розвитку електронного урядування в Україні. Науковий та інноваційний потенціал презентації : зб. наук. праць з матеріалами міжнар. наук.-практ. конф., м. Ополе, 18 листопада 2018 р. Рівне : «Волинські обереги», 2018. Т.6. С. 118-132.

18. Клименко І. В. Линьов К. О. Технології електронного урядування: Навчальний посібник. Київ: Вид-во ДУС, 2006. 225 с.

19. Клімушин П. С., Спасібов Д. В. Механізми електронного урядування в системі надання адміністративних послуг //Теорія та практика державного управління: зб. наук. праць. Харків : Вид-во ХарРІ НАДУ: Магістр. 2016. С. 50-55.

20. Клімушин П.С. Електронне урядування в інформаційному суспільстві : [монографія]. Харків : Вид-во ХарРІ НАДУ «Магістр», 2010. 312 с.

21. Клімушин П.С. Стратегії та механізми електронного урядування в інформаційному суспільстві : [монографія]. Харків : Вид-во ХарРІ НАДУ «Магістр», 2016. 524 с.

22. Ковбасюк Ю. В. Електронне врядування: європейський досвід та українські перспективи / Ю. В. Ковбасюк // Інвестиції: практика та досвід. 2010. № 16. – С. 81-83.

23. Литвинова Л.В. Менеджмент і маркетинг електронного урядування : навч. посіб. Київ : НАДУ, 2013. 68 с.

24. Лісовська Ю. П. Кібербезпека: ризики та заходи : навч. посіб. Київ : Видавничий дім «Кондор», 2019. С. 146-206

25. Літвінова Н. Проблеми надання адміністративних послуг громадянам із використанням інформаційно-комунікаційних технологій в Україні. Вітчизняний і зарубіжний досвід впровадження електронного урядування : зб. матеріалів наук.-практ. конф. Київ : НАДУ, 2018. С. 85-88.

26. Лобода С.М., Матвійчук-Юдіна О.В. Метод проектів у формуванні

27. компетентності з інфографіки у майбутніх бакалаврів з кібербезпеки. // Проблеми інженерно-педагогічної освіти: зб. наук, праць. 2017. № 54–55. С. 269–277.

28. Луцкий М. Г., Иванченко Е. В., Казмирчук С. В. Базовые понятия управления риском в сфере информационной безопасности /. // Захист інформації. 2001. №2. С. 86-94.

29. Мазур В. І. Інформаційні системи структури даних : навч.-метод. посіб. Київ : НАУ, 2007.

30. Мазур В. І. Тенденції розвитку інформаційних систем в міжнародному комунікаційному просторі. Науковий вісник Інституту міжнародних відносин НАУ. 2011. №1(3). С. 51-56.

31. Маракова І. Захист інформації: Підручник для вищих навчальних закладів/ Маракова І., Рибак А., Ямпольский Ю.,; Мін-во освіти і науки України, Одеський держ. політехнічний ун-т, Ін-т радіоелектроніки і телекомунікацій. Одеса, 2001. 164 с.

32. Моніторинг впровадження інструментів електронного урядування, як основи надання адміністративних послуг в електронному вигляді ; за. заг. ред. І.С. Куспляк, А.О. Серенок. Вінниця : ГО «Подільська агенція регіонального розвитку», 2016. 85 с.

33. Навчальний посібник/ розвиток електронного урядування на місцевому та регіональному рівнях./Київ, 2017 с. 16.

34. Нікітюк А.Р. Оцінювання розвитку електронного урядування в Україні. Управління. 2018. №4. С. 28–38.

35. Ніколіна І. І., Бондар М.В. Теоретичні засади оцінювання ефективності управління регіональним соціальним розвитком. Економіка. Фінанси.Менеджмент : актуальні питання науки і практики. 2017. №4(20). С. 63–71.

36. Орлов М. М. Удосконалення моделей електронного урядування в Україні //Видано за рішенням Вченої ради Харківського регіонального інституту державного управління Національної академії державного управління при Президентові України, протокол № 3/247-5 від 26 березня 2019 р. 2019. С. 151.

37. Петренко Л.Д. Основи електронного урядування. Харків : ХарРІ НАДУ, 2017. 312 с.

38. Рогозин Д. Война и мир в терминах и определениях / Рогозин Д. М.: Вече, 2016. 272 с.

39. Романенко Є. О. Інтернет як засіб комунікації та його вплив на формування державної політики. URL : http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/ape_2016_1_50.pdf

40. Семенченко А. І., Журавльов А. В. Теоретико-методологічні засади інституалізації державного управління у сфері електронного урядування [Електронний ресурс]. URL : http://www.academy.gov.ua/ej/ej14/txts/Semenchenko.pdf (дата звернення 17.03.2022).

41. Серенок А.О. Сервісна електронна взаємодія в системі електронного уряду. Актуальні проблеми державного управління : зб. наук. пр. Харків : ХарРІ НАДУ «Магістр», 2010. № 1 (37). С. 153–161.

42. Трухманов В. Світовий досвід електронної демократії. URL : http://www.cisp.org.ua/cisp/news.nsf/ b6be73c2257(дата звернення: 17.03.2022).

43. Чальцева О. Публічна політика: теоретичний вимір і сучасна практика /О.Чальцева /Вінниця. 2017. 244 с.

44. Чукут С.А, Загвойсько О.В. Інституційні та організаційні засади впровадження електронного урядування : кращі зарубіжні практики. Київ : НАДУ, 2011. 192 с.

45. Чукут С.А. Електронна демократія: сутність та основні етапи / Вітчизняний і зарубіжний досвід впровадження електронного урядування : зб. матеріалів наук.-практ. Конф. Київ : Вид-во НАДУ, 2018. С. 85-88.

46. Чукут С.А. Зарубіжний досвід упровадження електронного урядування. URL : http://derzhava.in.ua:8081/.pdf (дата звернення: 17.03.2022).

47. Чукут С.А. Проблеми та перешкоди на шляху електронного уряду : світовий та вітчизняний досвід. Державне управління в Україні : реалії та перспективи: зб. наук. пр. Київ : Вид-во НАДУ, 2015. С. 183-190.

48. Чукут С.А., Дмитренко В.І. Смарт-сіті чи електронне місто: сучасні підходи до розуміння впровадження е-урядування на місцевому рівні. Інвестиції: практика та досвід. № 13/2016. С. 89–93.

49. Швець М. Я. Україна на шлях у до інформаційного суспільства / М. Я. Швець, Р. А. Калюжний, В. С. Цимбалюк, В. Д. Гавловський та ін. Правова інформатика. 2011. №1. С. 90–99.

50. Юдін О. К. Інформаційна безпека держави / О. К. Юдін, В. М. Богуш. Харків: Консум, 2004. 508 с.

51. ChuanSheng R. E-Government Construction and China‘s Administrative Litigation Act [Text] / R. ChuanSheng // Electronic government: concepts, methodologies, tools and applications. New York : Information Science Reference, 2008. P. 988-993 (дата звернення 17.03.2022).

52. Delwit P. Electronic Voting in Belgium [Text] / P. Delwit, J.-B. Pilet, E. Kulahci // Electronic government: concepts, methodologies, tools and applications. New York : Information Science Reference, 2008. P.2749-2760.

53. Rohrig W. Cyber Security and Cyber Defense in the European Union / Rohig W. // Cyber Security Review 2014. №2. P.7-16

54. Wee G. Justice in the high-tech courts [Text] / G. Wee // Computer World. 2000. № 6 (40). P. 4-10.

55. Zhang N.N. From geographical space to composite space: The urban space under the influence of infor- mation networks [Text] / N.N. Zhang, C.L. Gu // Human Geography. 2002. № 17(4). P. 20-24.

56. eEurope – An information society for all [Text] / Communication on a commission initiative for the special European Council of Lisbon. Brussels, 2000. 16 p.

57. eEurope 2005: An information society for all [Text] / An Action Plan to be presented in view of the Sevilla European Council. Brussels, 2002. 22 p.

58. e-Japan Priority Policy Program [Electronic resource]. URL: http://www.kantei.go.jp/foreign/it/net- work/priority/index.html.

59. e-Japan Strategy [Electronic resource]. URL: http://www.kantei.go.jp/foreign/it/net- work/0122full_e.html.

60. Falch M. ICT as an Example of Industrial Policy in EU [Text] / M. Falch // Electronic government: concepts, methodologies, tools and applications. New York : Information Science Reference, 2008. P.1683- 1689.

61. Government of Japan (GOJ) [Electronic resource]. 2005. URL: http://www.guoukaku.go/jp/siryou/in- dex_kouhyou.html (дата звернення 17.03.2022).

62. Government of Japan (GOJ). Program for building e-government [Electronic resource]. 2003. URL: http://www.kantei.go.jp/jp/singi/it2/cio/dai4/4siryou2.pdf (дата звернення 17.03.2022).

63. Henten A. European planning for an information society [Text] / A. Henten, M. Falch, K. Skouby // Telematics and Informatics. 1996. № 13(2). P. 177-190.

64. i2010 – A European information society for growth and employment [Electronic resource]. 2005. URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52005DC0229 (дата звернення 17.03.2022).

65. Kubo S. Local E-Governement in Japan: IT Utilization Status and Directions [Text] / S. Kubo, T. Shimada // Electronic government: concepts, methodologies, tools and applications. New York : Information Science Reference, 2008. P. 2217-2230.

66. Leitner C. E. Government in Europe: The State of Affairs [Text] / C. Leitner. Maastricht : European Institute of Public Administration, 2003. 63 p.

67. Lisbon Strategy [Electronic resource]. URL: http://cordis.europa.eu/programme/rcn/843_en.html (дата звернення 17.03.2022).

68. Lu Z. The Development of Urban E-Governement in China [Text] / Z. Lu, J. Zhang, B. Han, Z. Deng, J. Lu // Electronic government: concepts, methodologies, tools and applications. New York : Information Science Reference, 2008. P.655-675.

69. Memorandum on Electronic Government [Electronic resource]. 1999. URL: http://www.gpo.gov/fdsys/pkg/PPP-1999-book2/pdf/PPP-1999-book2-doc-pg2317.pdf (дата звернення 17.03.2022).

70. Ministry of Public Management, Home Affairs, Posts and Telecommunication [Electronic resource]. 2005. URL: http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2004/2004-index.html (дата звернення 17.03.2022).

71. Next Generation of e-Government for Developing Countries: Lessons Learned from the Cases of the EU and Korea [Electronic resource]. URL: http://www.computer.org/portal/web/csdl/doi/10.1109/ICCIT.2008.395 (дата звернення 17.03.2022).

72. Seifert J.W. E-Government Act of 2002 in the United States [Text] / J.W. Seifert, H.C. Relyea // Elec- tronic government: concepts, methodologies, tools and applications. New York : Information Science Reference, 2008. P. 154-161 (дата звернення 17.03.2022).

73. Singapore E-government Action Plan [Electronic resource]. URL: http:/unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN002999.pdf (дата звернення 17.03.2022).

74. Some key issues in Europe‘s competitiveness – Towards an integrated approach [Electronic resource]. 2005. URL: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52003DC0704 (дата звернення 17.03.2022).

75. The Role of eGovernment for Europe's Future [Text]. Brussels : Commission of the European communities, 2003. 26 p.

76. The U.S.A. Government's Official Web Portal [Electronic resource]. URL: http://www.usa.gov (дата звернення 17.03.2022)