НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

КОТУХ Євген Володимирович

УДК 35.085:316.344.42

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ПУБЛІЧНОМУ СЕКТОРІ

25.00.02 – механізми державного управління

РЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора наук з державного управління

Харків – 2022

Дисертацією є рукопис.
Робота виконана в Національному університеті цивільного захисту України.

Офіційні опоненти:

доктор наук з державного управління, доцент
ТОРІЧНИЙ Вадим Олександрович,
професор кафедри національної безпеки та управління факультету підготовки керівних кадрів Національної академії Державної прикордонної служби України

доктор наук з державного управління, доцент
ЩЕПАНСЬКИЙ Едуард Валерійович,
завідувач кафедри публічного управління та адміністрування Хмельницького університету управління та права імені Леоніда Юзькова

доктор наук з державного управління, доцент
КАРПЕНКО Олександр Валентинович,
завідувач кафедри національної економіки та публічного управління Державного вищого навчального закладу «Київський національний економічний університет імені Вадима Гетьмана»

Захист відбудеться «05» жовтня 2022 р. о 11.00 годині на засіданні спеціалізованої вченої ради Д 64.707.03 Національного університету цивільного захисту України за адресою: 61024, м. Харків, вул. Лермонтовська, 28, ауд. 4 (1-й поверх).

З дисертацією можна ознайомитись у бібліотеці Національного університету цивільного захисту України за адресою: 61023, м. Харків, вул. Чернишевська, 94.

Учений секретар
спеціалізованої вченої ради С.А. Мороз

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Забезпечення кібербезпеки на даний час є важливою проблемою на всіх рівнях публічного управління: від місцевих органів влади, що займаються онлайн-транзакціями, до центральних органів влади, що займаються питаннями національної безпеки. Кібербезпека – це динамічна мета, яка змінюється з такою швидкістю, що дуже важко отримати абсолютно актуальне уявлення про неї. Нові кіберзагрози або варіації старих виникають майже щодня, як і стратегії захисту від них. Однак існують і деякі загальні підходи до забезпечення кібербезпеки, які слід визначати та адаптувати до специфіки конкретних держав і конкретних органів публічної влади.

Забезпечення кібербезпеки занадто часто віддають ІТ-фахівцям, які погано розбираються в більших організаційних проблемах або виробленні політики, в той час як вище керівництво публічних організацій не розуміє пов'язаних з цим технічних питань. Тому важливим завданням є переведення новітніх технічних термінів і загроз у поняття, зрозумілі для вищого керівництва, співробітників і суспільства в цілому. Усунення розриву між ІТ-фахівцями і керівниками публічного сектора й особами, що визначають політику, має фундаментальне значення для підвищення кібербезпеки.

Крім того, організації публічного сектора можуть створити більш сильний кіберзахист, налагоджуючи більш тісні відносини і співпрацюючи з іншими для обміну досвідом, помилками, отриманими уроками та іншою інформацією і дослідженнями. Готовність збирати, аналізувати й обмінюватися інформацією, в тому числі про кіберінциденти, має вирішальне значення для підвищення загального рівня кібербезпеки. А це потребує налагодження співпраці з вітчизняними та міжнародними акторами з усіх трьох секторів: публічного, приватного, неурядового, що, зокрема, дозволить підвищити суспільну обізнаність щодо кіберзагроз, їх небезпек і методів запобігання.

Зовнішня і внутрішня ефективність публічного сектора може значно підвищитися за рахунок використання нових інформаційно-комунікаційних технологій, проте сучасні тенденції в цій сфері можуть також призвести до появи нових викликів та нових проблем. Очевидно, що частота і масштаби кібератак будуть збільшуватися, в тому числі й на публічний сектор. Шкідливе ПЗ, інсайдерські робочі місця, бот-мережі, DDoS-атаки, кібершпіонаж і кібертероризм ставатимуть все більш витонченими і, як і раніше, наноситимуть фінансову, репутаційну та інші види шкоди, а також створювати загрозу національній безпеці. Тому у даний час кібербезпека – це глобальна проблема, яка потребує глобальної відповіді, але це також локальна проблема, що вимагає локального реагування. Відтак, кожна сучасна публічна організація зобов'язана проявляти ініціативу і реалізовувати політики, що підвищують рівень кібербезпеки. Від цього залежить не тільки її власна безпека, але і безпека всього публічного сектора, держави і суспільства в цілому.

Теоретико-методологічні засади публічного управління в сучасних умовах висвітлюються в працях таких науковців, як В. Бакуменко, Д. Белл, Т. Бове, Е. Гідденс, В. Дзюндзюк, М. Дрепо, М. Кастельс, В. Князєв, Ю. Куц,

М. Лахижа, Е. Лоффлер, М. Маклюен, Дж. Най, С. Попов, К. Торнхілл, П. Уілбі, Р. Хікс, В. Шамрай та ін.

Питання формування та реалізації державної політики щодо забезпечення кібербезпеки розглянуто у працях таких зарубіжних дослідників, як М. Данн, К. Зеттер, Дж. Карр, С. Кемпбелл, Р. Кларк, Е. Клімбург, Р. Кнейк, М. Лібіцкі, Т. Мур, П. Розенцвейг, Т. Стівенс, Дж. Хілі, Р. Хьюс та ін.

Серед вітчизняних науковців проблеми забезпечення інформаційної та кібербезпеки у публічному секторі досліджували такі науковці як М. Бутко, С. Гончар, Ю. Даник, П. Воробієнко, Б. Дзюндзюк, Д. Дубов, В. Карпенко, Б. Корнієнко, О. Курбан, В. Лизанчук, Ю. Лісовська, Р. Лук'янчук, О. Орлов, Г. Почепцов, О. Рижук, А. Семенченко, Т. Станіславський, В. Степанов та ін.

Проте проблема забезпечення кібербезпеки у публічному секторі залишається недостатньо розробленою. Насамперед це стосується напрацювань, присвячених методологічним підходам до практичної реалізації теоретичних моделей і концепцій у даній сфері. Також бракує праць, присвячених адаптації вже наявного позитивного досвіду як до специфіки конкретних країн, так і з урахуванням нових викликів, що постійно виникають у кіберпросторі. Усе це зумовлює актуальність теми дисертації, визначає її мету й завдання.

Зв'язок роботи з науковими програмами, планами, темами. Тема дисертаційної роботи пов'язана з науково-дослідними роботами «Публічне управління в умовах глобалізації» (державний реєстраційний номер 0220U104528) та «Євроінтеграційний вектор розвитку України та реалізація національних інтересів в умовах глобальних викликів» (державний реєстраційний номер 0120U105649), що виконувались кафедрою політології та філософії Харківського регіонального інституту державного управління Національної академії державного управління при Президентові України. У межах першої теми автором визначено особливості забезпечення кібербезпеки у середовищі Gov 2.0, другої – основні виклики для публічного сектора у контексті забезпечення кібербезпеки.

Мета і задачі дослідження. Метою дослідження є теоретико-методологічне обґрунтування забезпечення кібербезпеки в публічному секторі в сучасних умовах.

Досягнення визначеної мети зумовило необхідність вирішення таких *завдань*:

– розкрити зміст і особливості електронного врядування як парадигми публічного управління;

– з'ясувати основні виклики для публічного сектора у контексті забезпечення кібербезпеки;

– обґрунтувати концептуальні засади забезпечення кібербезпеки в органах публічної влади;

– визначити основні принципи інституційної кібербезпеки в публічному секторі;

– узагальнити зарубіжні практики щодо забезпечення кібербезпеки у

публічному секторі;

– з’ясувати особливості запобігання та протидії кіберзагрозам у публічному секторі України;

– обґрунтувати методологічний підхід до забезпечення кібербезпеки у середовищі Gov 2.0;

– з’ясувати використання різних типів владних відносин у забезпеченні кібербезпеки;

– розробити модель інституційної кібербезпеки, визначити її основні компоненти;

– обґрунтувати теоретико-методологічну модель розробки національної стратегії кібербезпеки;

– розглянути особливості публічно-приватного партнерства у сфері забезпечення кібербезпеки.

Об’єкт дослідження – формування та реалізація державної політики у сфері кібербезпеки.

Предмет дослідження – забезпечення кібербезпеки в публічному секторі в сучасних умовах.

Методи дослідження. Методологічною основою дослідження є системний підхід, що дозволяє представити державну політику стосовно забезпечення кібербезпеки як складну структурно-організовану систему, яка потребує удосконалення та розвитку. Для досягнення мети й завдань дисертаційного дослідження використовувався комплекс загальнонаукових і спеціальних методів, зокрема:

– історико-генетичний, логіко-семантичний, аналіз, узагальнення, ідеалізація (розкриття змісту й особливостей електронного врядування як парадигми публічного управління);

– історико-генетичний, логіко-семантичний, узагальнення, абстрагування, порівняння (з’ясування основних викликів для публічного сектора у контексті забезпечення кібербезпеки);

– системний, абстрагування, порівняння, формалізація, історико-генетичний, інституціональний аналіз (обґрунтування концептуальних засад забезпечення кібербезпеки в органах публічної влади);

– історико-генетичний, логіко-семантичний, класифікації, узагальнення, аналіз, формалізація, порівняння (визначення основних принципів інституційної кібербезпеки в публічному секторі);

– емпіричний, абстрагування, порівняльний аналіз, узагальнення, описово-індуктивний, спостереження (узагальнення зарубіжних практик щодо забезпечення кібербезпеки у публічному секторі);

– емпіричний, індукція, узагальнення, синтез, діалектичний, прогностичний (з’ясування особливостей запобігання та протидії кіберзагрозам у публічному секторі України);

– діалектичний, індукція, узагальнення, формалізація, прогностичний (обґрунтування методологічного підходу до забезпечення кібербезпеки у середовищі Gov 2.0);

– системний, діалектичний, інституціональний аналіз, факторний аналіз (з'ясування використання різних типів владних відносин у забезпеченні кібербезпеки);

– моделювання, системний, інституціональний аналіз, узагальнення, формалізація, синтез (розробка моделі інституційної кібербезпеки);

– моделювання, системний, діалектичний, узагальнення, формалізація, синтез (обґрунтування теоретико-методологічної моделі розробки національної стратегії кібербезпеки);

– системний, індукція, узагальнення, порівняння, інституціональний аналіз, структурно-функціональний аналіз (розгляд особливостей публічно-приватного партнерства у сфері забезпечення кібербезпеки).

Крім зазначених методів дослідження у дисертації широко використовувалися такі методи дослідження як аналіз статистичних даних і офіційних документів, а також порівняльно-правовий та компаративний методи, використання яких мало суцільний характер.

Теоретичну основу роботи складають наукові праці фахівців у галузі науки державного управління, соціології, політології, юридичних наук. Особливе місце у дисертації приділено аналізу спеціальної літератури з тематики дослідження: статей у спеціалізованих наукових виданнях, монографій, енциклопедій, словників.

У дисертації широко використана нормативно-правова база України та інших країн, які регулюють різні аспекти формування та реалізації державної політики щодо забезпечення кібербезпеки у публічному секторі. При написанні роботи використано вітчизняні та зарубіжні джерела (довідкові видання, статистичні матеріали тощо), які послужили інформаційною та емпіричною основою для вирішення визначених завдань дослідження.

Наукова новизна одержаних результатів полягає в обґрунтуванні теоретико-методологічних положень і визначенні практичних заходів щодо забезпечення кібербезпеки в публічному секторі в сучасних умовах.

Найважливіші наукові результати дисертаційного дослідження розкриваються в таких положеннях:

уперше:

– обґрунтовано концептуальні засади забезпечення кібербезпеки в органах публічної влади, які поділяються на дві групи: виміри кібербезпеки (людський, організаційний, інфраструктурний, технологічний, нормативний) та дії, необхідні для забезпечення кібербезпеки (побудова онлайн-довіри; розвиток координації, співпраця та кооперація; профілювання кіберстану; сприяння впровадженню систем кібербезпеки; перегляд; створення правового середовища; встановлення стандартів);

– розроблено модель інституційної кібербезпеки, відповідно до якої інституційна кібербезпека повинна мати такі основні компоненти: політика, стратегія та стандарти з кібербезпеки; управління кіберризиками; управління вразливістю та загрозами; централізоване управління інцидентами; поінформованість про кібербезпеку та освіта; управління логами та кореляція; безпечна архітектура; правові норми; технічні інструменти; безперервність

діяльності; постійний аудит та моніторинг; співпраця; кіберстійкість;

– обґрунтовано теоретико-методологічну модель розробки національної стратегії кібербезпеки, яка використовує підходи неореалізму, соціального конструктивізму, інтерсекційності, кібервестфалізму та враховує, що актори у кіберпросторі (державні актори, недержавні актори, кінцеві користувачі та кіберзлочинці) здійснюють дії (проводять політику, слідують політиці, атакують, захищаються від нападів, отримують і передають інформацію, здійснюють комунікацію, використовують інформаційно-комунікаційні технології для роботи й у побуті тощо), які перетинаються з різними аспектами кіберпростору та кібербезпеки (політичними, соціальними, культурними, технологічними) та породжують явища кібербезпеки, такі як вразливості, цілісність системи, шкідлива поведінка, ідентичність, мотивація тощо;

удосконалено:

– методологічний підхід до забезпечення кібербезпеки у середовищі Gov 2.0, визначено, що вона має ґрунтуватись на реалізації таких заходів: модерування контенту публічних аккаунтів; запобігання несанкціонованому використанню і передачі конфіденційної інформації; використання браузерів з обмеженими привілеями; впровадження систем виявлення / запобігання вторгнень; використання сервісів Web-репутації; фільтрація універсального локатора ресурсів (URL) та Інтернет-протоколу (IP); фільтрація шкідливих програм по периметру мережі; використання інструментів попереднього перегляду скорочення URL;

– перелік основних принципів інституційної кібербезпеки, до яких віднесено такі: запровадження холістичного підходу до кібербезпеки; використання гнучкого стилю управління у сфері кібербезпеки; впровадження методів постійного вдосконалення діяльності, орієнтованих на управління ризиками; віднесення до базису забезпечення кібербезпеки координації діяльності публічних, приватних, академічних та неурядових організацій разом з міжнародною співпрацею та обміном інформацією; заохочення прозорості, підзвітності, етичних цінностей, свободи слова у кіберпросторі; встановлення балансу між безпекою та застосовністю ІТ-продуктів і технологій;

– обґрунтування основних принципів публічно-приватного партнерства у сфері забезпечення кібербезпеки, до яких віднесено такі: перехід від «класичного» партнерства до взаємовигідної співпраці; визначення ролей членів партнерства за допомогою підходів управління ризиками; запровадження спільної відповідальності членів партнерства щодо загроз і вразливостей; впровадження системи оцінювання партнерства;

дістали подальшого розвитку:

– концептуальні положення щодо трактування кібербезпеки як суспільного блага; було визначено, що кібербезпека, маючи три основні складові (інформаційно-комунікаційні системи, які є надійними і можуть протистояти атакам; методи та системи виявлення загрози та аномалій для забезпечення стійкості інформаційно-комунікаційних систем; забезпечення системної реактивності на кібератаки), забезпечує задоволення публічних інтересів інформаційного суспільства щодо можливості належного

функціонування критично важливих національних інфраструктур і дозволяє громадянам здійснювати свою рутинну діяльність, спираючись на безпечні технології;

– визначення основних викликів для публічного сектора у контексті забезпечення кібербезпеки, до яких віднесено такі: 1) велика ступінь оперативної незалежності та «ізольованості» між різними частинами публічного сектора, що робить для нього вирішення питань кібербезпеки набагато більш складним ніж для приватного; 2) важливі загальнодоступні дані створюються, зберігаються та застосовуються відповідними суб'єктами поза органами публічної влади; 3) працівники організацій публічного сектора далеко не завжди демонструють безпечну поведінку у кібепросторі, хоча саме поведінка людини є стрижнем кібербезпеки; 4) зворотна залежність між використанням інформаційно-комунікаційних технологій і кібербезпекою; 5) відсутність або неефективність публічно-приватного партнерства щодо забезпечення кібербезпеки;

– узагальнення зарубіжних практик щодо забезпечення кібербезпеки у публічному секторі, зокрема, з'ясовано, що сфера кібербезпеки вже включена до порядку денного з питань безпеки всіх досліджених держав, але дана сфера у різних державах відрізняється за тим, як держави, по-перше, визначають референтний об'єкт (що потрібно захищати), по-друге, сприймають основні загрози та ризики та, по-третє, визначають джерела загроз та ризики; відповідно до цих відмінностей держави можна поділити на дві категорії: держави, що мілітаризують питання кібербезпеки, та держави, що криміналізують питання кібербезпеки;

– методологічний підхід до використання різних типів владних відносин у забезпеченні кібербезпеки; визначено, що примусова влада стосовно кібербезпеки надає можливості для безпосереднього контролю одного актора з боку іншого; інституційна влада надає можливість опосередкованого контролю над акторами за посередництва інститутів; структурна влада визначає соціальні можливості та інтереси шляхом реалізації державно-приватних партнерських відносин; продуктивна влада дає можливість з'ясувати, яким чином системи знань та дискурсивні практики функціонують у мережах соціальних сил, породжених кіберпростором;

– визначення особливостей запобігання та протидії кіберзагрозам у публічному секторі України, зокрема, визначено комплекс взаємопов'язаних заходів, які передбачають збільшення рівня кібербезпеки в публічному секторі, що включають: організаційну (створення в органах публічної влади спеціальних підрозділів), матеріально-технічну (установка сучасного обладнання і програмного забезпечення), кадрову (підвищення кваліфікації управлінських кадрів з питань кібербезпеки) і бюджетно-фінансову складову (виділення в державному і місцевому бюджетах обов'язкового цільового фінансування зазначених заходів).

Практичне значення одержаних результатів полягає в можливості їх використання в діяльності органів влади, що сприятиме підвищенню ефективності діяльності як окремих органів влади, так і системи публічного

управління в цілому.

Розроблені автором рекомендації щодо підвищення кібербезпеки впроваджено в діяльність:

– Міністерства фінансів України (довідка від 20 серпня 2021 р. № 20040-03-73/26056);

– Міністерства молоді та спорту України (довідка від 13 липня 2021 р. № 6090/1);

– Державної аудиторської служби України (довідка від 13 липня 2021 р. № 001400-16/8764-2021).

Особистий внесок здобувача. Дисертація є самостійно виконаною науковою працею. Усі сформульовані в ній висновки, теоретичні положення та пропозиції ґрунтуються на особистих дослідженнях. У дисертації не використовувалися ідеї співвиконавців науково-дослідних робіт.

Апробація результатів дослідження. Основні положення та результати дисертаційної роботи викладено в наукових повідомленнях на комунікативних заходах: XX Міжнародний науковий конгрес «Публічне управління XXI століття: портал можливостей» (м. Харків, 2020 р.), XXI Міжнародний науковий конгрес «Публічне управління XXI століття: погляд у майбутнє» (м. Харків 2021 р.), International Scientific Integration ‘2020 (Seattle, Washington, USA, 2020), IV International Scientific Conference «Science and Global Studies» (Prague, 2020), 7th International Conference on Internet of Things: Systems, Management and Security (Paris, France, 2020), Multidisziplinare Forschung: Perspektiven, Probleme und Muster (Wien, 2021), 18-та регіональна науково-практична конференції «Актуальні проблеми європейської та євроатлантичної інтеграції України» (м. Дніпро, 2021 р.) та ін.

Публікації. Основні положення дисертаційного дослідження висвітлено у 30 публікаціях, з них 1 – одноосібна монографія, 3 – статті у наукових періодичних виданнях, проіндексованих у базах даних Web of Science Core Collection та Scopus, 19 – статті у наукових фахових виданнях у галузі науки «Державне управління».

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, п’яти розділів, висновків, списку використаних джерел і додатку. Її повний обсяг становить 479 сторінок, у тому числі: рисунків – 80 (на 35 сторінках), таблиць – 13 (на 17 сторінках), додатків – 1 (на 3 сторінках). Список використаних джерел налічує 530 найменувань (на 56 сторінках), у тому числі іноземною мовою – 301.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **першому розділі – «Особливості інформаційного суспільства, що впливають на кібербезпеку»** – розкриваються зміст і особливості електронного врядування як парадигми публічного управління, визначається поняття і сутність кібербезпеки у публічному секторі, розглядаються особливості впровадження систем кібербезпеки в органах публічної влади.

З’ясовано, що відсутність ефективних заходів з кібербезпеки може

потенційно вплинути на інформаційну революцію та розвиток інформаційного суспільства по всьому світу. Без відповідних заходів безпеки кіберзагрози можуть підірвати стабільність інформаційних суспільств, зробивши цифрові технології джерелом ризиків, а не лише джерелом розвитку. Крім того, відсутність безпеки цифрових технологій зруйнує довіру користувачів до них, а це, у свою чергу, завадить впровадженню інновацій, насамперед, у публічному секторі. Створення надійних інформаційно-комунікаційних систем має прямі та непрямі наслідки для публічних інтересів інформаційного суспільства, оскільки це дає можливість належного функціонування критично важливих національних інфраструктур, і дозволяє громадянам здійснювати свою рутинну діяльність, спираючись на безпечні технології. Це дає підстави стверджувати, що кібербезпека є суспільним благом.

Визначено, що три важливі переваги випливають із управління кібербезпекою як суспільним благом: системний підхід до безпеки; спільна відповідальність між різними стейкхолдерами; розвиток співпраці у сфері кібербезпеки. Що стосується системного підходу, то управління суспільним благом вимагає розгляду як прямих, так і непрямих зовнішніх чинників, а також середньо- і довгострокових наслідків. Це сприяє використанню підходів, спрямованих на визначення та аналіз взаємозалежностей щодо безпеки різних, але пов’язаних, технологій та їх впливу на різні суспільні сфери. Стосовно спільної відповідальності: управління суспільним благом вимагає співробітництва між приватним і публічним сектором в цілях забезпечення високого рівня надійності відповідних систем та інфраструктур. Публічний сектор насамперед повинен встановлювати стандарти, здійснювати сертифікацію та тестування, процедури нагляду, щоб забезпечити підтримання достатнього рівня кібербезпеки для захисту та сприяння суспільним інтересам, а також вживати відповідних заходів, коли кібербезпека не забезпечується належним чином. У той же час, приватний сектор несе відповідальність за розробку надійних систем, розробку та вдосконалення методів забезпечення надійності послуг та продуктів, які вони пропонують, та співпрацює з публічним сектором для здійснення відповідного контролю. Визначення кібербезпеки як суспільного блага також покладає на користувачів певні обов’язки щодо їх кібергігієни. При цьому розподіл відповідальності між різними акторами, а також необхідність врахування прямих та непрямих зовнішніх ефектів сприяє співпраці та обміну інформацією. Обмін інформацією про уразливість різних систем, наприклад, є важливим для приватного сектора для гарантування надійності інформаційно-комунікаційних системи. У той же час, публічний сектор може підтримувати цю практику, включаючи обмін інформацією та співпрацю як частину ініціатив та процедур щодо підвищення власної спроможності.

Виявлено, що кібербезпека охоплює широкий набір практик: оцінка ризиків і тестування проникнення; аварійне відновлення; криптографія; контроль та спостереження за доступом; мережева архітектура, програмне забезпечення та безпека; безпекові операції; фізична безпека тощо. При цьому кібербезпека має три основні складові: 1) інформаційно-комунікаційні системи,

які є надійними і можуть протистояти атакам; 2) методи та системи виявлення загрози та аномалій для забезпечення стійкості інформаційно-комунікаційних систем; 3) забезпечення системної реактивності на кібератаки. Причому щоб зрозуміти кібербезпеку в публічному секторі, слід усвідомити конвергенцію трьох основних чинників: глобалізації, ступеню підключення до мережі та тенденції до надання послуг публічному сектора в Інтернеті, що зазвичай називають електронним урядом (е-урядом).

Показано, що реформування публічного управління, частиною якого є впровадження електронного врядування, можна спостерігати як загальносвітову тенденцію, що простежується у багатьох країнах. І це не просто експерименти щодо впровадження нових режимів надання послуг, оскільки електронне врядування неминуче також охоплює (і керується) новими моделями формування політики, новими моделями участі громадян у публічному управлінні та політичних процесах, новими моделями відносин громадян і влади, новими варіантами соціально-економічного розвитку. При цьому електронне врядування слід розглядати як самостійну парадигму публічного управління, оскільки впровадження ІКТ суттєво змінило його характер. Це вірно, як з точки зору внутрішньої діяльності органів влади (G2G), так і з точки зору їх взаємодії з іншими стейкхолдерами (G2C та G2B). Слід визнати і те, що електронне врядування сильно впливає на розвиток і в інших галузях, таких як інформаційно-комунікаційні технології та електронна комерція, які у свою чергу впливають на електронне врядування.

Визначено, що кіберзагрози можна класифікувати декількома способами, один з яких – порівняння політично вмотивованих загроз (наприклад, кібервійна, кібертероризм, кібершпигунство та хактивізм – хакерство в політичних цілях) із неполітичними (зазвичай фінансово мотивованими, як то кіберзлочин, крадіжка інтелектуальної власності та шахрайство, а також злам для розваги чи відплати, наприклад, від незадоволеного працівника). Ще один спосіб класифікації кіберзагроз – за тим, чи є вони зовнішніми або внутрішніми по відношенню до об’єкта впливу.

З’ясовано, що поширення використання ІКТ, поза сумнівом, означає, що публічний сектор має усвідомити та докласти зусиль, щоб уникнути одночасної втрати знань та контролю над основними процесами (та компетенціями, рішеннями та політикою, необхідними для їх підтримки), які є основою надання всіх державних послуг. Необхідно краще зрозуміти, які аспекти діяльності публічного сектора можуть і повинні бути кодифіковані, «товаризовані» (наприклад, за допомогою ІКТ) та передані в аутсорсинг або «підключені до мережі» з іншими суб’єктами, включаючи приватний та громадський сектори, і, як все більше здається, включаючи користувачів. Ті, що мають приймати рішення, поки що не долучаються до всіх цих питань, але в умовах, коли уряди намагаються скоротити витрати, значення цих питань знову різко зростає. І хоча очевидно, що широке оприлюднення даних публічного сектору може принести величезні переваги, майже напевно існують законні інтереси, які слід захистити від повної прозорості та відкритості. Наприклад, існують, безперечно, законні потреби та інтереси приватності громадян та

підприємств, коли їхні дані використовуються органами влади. Однак настільки ж важливими є й інтереси публічних службовців та політиків, особливо під час процесу прийняття рішень та політичної діяльності, наприклад, у захисті від настирливого впливу та моніторингу, які можуть стати наслідком того, що всі їх дії та рішення стають абсолютно прозорими. Це може спричинити стрес та надлишкову зосередженість на вимірюванні та виконанні обов'язків на особистому рівні та призвести до надто бюрократичної позиції, роботи суворо за правилами замість того, щоб бути гнучкими та готовими сприймати вимірний ризик політичних ідей. Це також може спровокувати небажання приймати рішення або брати на себе відповідальність за них.

Виявлено, що активна розробка та впровадження систем кібербезпеки (СКБ) на різних рівнях почались з початку 2000-х років. При цьому загальні принципи та основні особливості таких систем кібербезпеки знайшли відображення у низці керівних документів. Певні особливості та відмінності можуть бути знайдені в кожній СКБ, адже кожна СКБ у певному сенсі є унікальною, і аналіз керівних документів з впровадження СКБ дав можливість визначити чотири аспекти такої унікальності, а саме: 1) заохочувані дії; 2) драйвери; 3) середовище та 4) аудиторія. При цьому, заохочувана дія – це бажана чи рекомендована дія, що пов'язана з основним змістом СКБ; драйвер є фактором, що мотивував створення даної СКБ; середовище – це ситуаційні обставини, в яких можна використовувати СКБ; аудиторія – ймовірні користувачі СКБ. Виходячи із цього було обґрунтовано концептуальні засади забезпечення кібербезпеки в органах публічної влади (рис. 1).

З'ясовано, що життєвий цикл СКБ складається з трьох загальних етапів: профілювання кіберстану, досягнення встановлених цілей кібербезпеки та оцінювання. Причому результати оцінювання на останньому етапі використовуються для уточнення кіберстану і удосконалення стратегії кібербезпеки. Процес профілювання призначений для визначення поточного кіберстану, і у загальному випадку профілювання можна визначити як процес планування, що містить визначення припущень, узгодження запланованих дій з основними цінностями, формування бюджету, визначення необхідних ресурсів та створення правового середовища. Досягнення встановлених цілей кібербезпеки є основним засобом захисту кіберпростору. Цей процес повинен здійснюватися на основі припущень, визначених в процесі профілювання. Оцінювання передбачає огляд і аналіз процесу досягнення та отриманих результатів, у тому числі з використанням зворотного зв'язку. Оцінювання тягне за собою перегляд, уточнення і модифікацію стратегії кібербезпеки та СКБ у цілому.

У другому розділі – «Сучасні тенденції і підходи до забезпечення кібербезпеки у публічному секторі» – здійснюється аналіз сучасних тенденцій і підходів до забезпечення кібербезпеки у публічному секторі крізь призму зарубіжного досвіду.

З'ясовано, що проблема зростання кількості кібератак на мережі та ускладнення їх характеру робить питання кібербезпеки все більш актуальнішим. Нові агресивніші форми кіберактивності та поява неурядових

акторів у якості активних учасників процесів визначення внутрішньої та зовнішньої політики викликають численні запитання про майбутнє публічного сектору з точки зору забезпечення національного суверенітету та незалежності.

Рис. 1. Концептуальні засади забезпечення кібербезпеки в органах публічної влади

Широкий діапазон потенційних загроз створює серйозні виклики існуючим міжнародним структурам, які часто не встигають за кіберпростором, що динамічно розвивається. Водночас, політика, яка націлена проти різних загроз у кіберпросторі, зазвичай розвивається ізольовано, що призводить до невідповідностей та відсутності узгодженості рішень, що ухвалюються окремими урядами. Отже, глобальним кіберзагрозам протиставляються локальні рішення, які часто не встигають за технологіями та тенденціями розвитку кіберзлочинності. Таким чином, постає питання визначення цих тенденцій, оцінка їх значення для окремих держав, а також розробка конкретних пропозицій щодо системного протистояння цим загрозам.

Встановлено, що у міжнародних наукових та політичних колах протягом останніх років сформувалась певна спільна думка щодо наступних позицій. По-перше, всі (більшість держав та їх громадян) згодні, що життєдіяльність людства залежить від мережі, а інформаційні технології – це ключ до подальшого соціального та економічного розвитку. По-друге, на практиці це

перетікає у зростаюче визнання того, що залежність життя у XXI сторіччі від інформаційної інфраструктури робить всіх (як окремих громадян, так і різноманітні установи, організації, підприємства і навіть цілі країни) надзвичайно вразливими до кіберзагроз. По-третє, потенційні загрози є досить серйозними, враховуючи залежність від мережі та відомих випадків вразливості кіберпростору, проте наразі сучасні державі не готові боротися з кіберзагрозами; атаки трапляються все частіше, а наслідки все триваліші. По-четверте, згідно з дослідженнями конкретних випадків та висновками, всі держави вразливі до переворотів, програми у сфері атомної енергетики вразливі до кібератак, а витоки інформації та революції через «Facebook» можуть нашкодити державам та дипломатичним відносинам між ними. Необхідно вживати певних заходів для того, щоб цифрове життя та інтереси стали безпечнішими. Визнання характеру та масштабу проблеми – це перший крок до її вирішення у майбутньому. По-п’яте, кіберпростір являє собою «справжню», відносно нову сферу взаємодії (як місцевої, так і міжнародної), яка є такою ж важливою, як і взаємодія у повітрі, на морі, на суші та в космосі. Кіберпростір заслуговує на той же рівень взаємодії, захисту і уваги, як і будь-яка інша сфера.

Визначено, що серйозним викликом для національних урядів є обмежена кількість ресурсів. З одного боку, варто визнати, що витрати на кібербезпеку у національних бюджетах щороку зростають. З іншого боку – кібербезпека коштує достатньо дорого, а враховуючи, що наразі бюджети на національну оборону підлягають безперервному перегляду, можливості для гідного протистояння кіберзагрозам постійно зменшуються. Таким чином, обґрунтування виділення ресурсів на кібербезпеку, що зазвичай сприймається більшістю науковців та політиків як боротьба з гіпотетичною загрозою, (враховуючи обмежену кількість точних даних про конкретні результати інвестицій у цю сферу) – представляється достатньо складним завданням. Ускладнює ситуацію і те, що зазвичай через недостатню прозорість уряди і приватні компанії не бажають розкривати всю інформацію про атаки на їх активи. Таким чином, спільна проблема публічного та приватного секторів полягає у пошуку інвестицій, необхідних для покращення стандартів безпеки.

З’ясовано, що у відповідь на наявні загрози держави у всьому світі розробляють стратегії кібербезпеки, зазвичай – шляхом створення певного національного правового акту або програми для реагування на кіберзагрози та захисту найважливіших мереж. Однак пріоритети стратегій національної безпеки різних держав відрізняються. Деякі держави мають чітке уявлення про кіберсередовище та його головні референтні об’єкти, такі як критична інфраструктура, і, відповідно, сформували комплексний підхід до сприйняття проблем, що становлять загрозу для кібербезпеки та національної безпеки, та визначили найважливіші джерела цих загроз. Унаслідок цього, ключовою умовою для реалізації ефективних стратегій кібербезпеки у цих країнах є призначення державних відомств відповідальними за управління кібербезпекою. З іншого боку, держави, в яких переважає цивільний підхід до кібербезпеки, зосереджуються переважно на боротьбі з кіберзлочинністю. Потенційні джерела загроз кіберзлочинності не визначені чітко і пов’язані,

переважно, з приватною власністю і належним функціонуванням сектору економіки. Але при цьому, як показує аналіз, стратегії кібербезпеки більшості держав зосереджують увагу на п’яти основних сферах: 1) військові кібероперації; 2) розвідка і контррозвідка; 3) боротьба з кіберзлочинністю; 4) захист критичної інфраструктури та врегулювання кризових ситуацій; 5) кібердипломатія та управління Інтернетом.

Було визначено дві парадигми, що стосуються забезпечення кібербезпеки у публічному секторі. Першою є так звана державницька парадигма, яка відображає традиційну роль держави в захисті кордонів та забезпеченні верховенства права У межах цієї парадигми кібербезпека вважається фундаментальним фактором воєнної та економічної безпеки держави, і тому до неї застосовуються традиційні аргументи національної безпеки, що базуються на захисті батьківщини. Інакше кажучи, цей підхід підкреслює зв’язок між захистом критичної інфраструктури і тих державних та приватних систем, що є важливими для функціонування держави. Державницька парадигма відноситься до традиційного підходу до управління та запобігання ризикам з кіберпростору у спосіб, що може спричинити зростання впливу військових сил у сфері стратегій кібербезпеки. Другою є економічна парадигма, яка відображає зростання впливу інтернету на економічний добробут держави. Тим часом як державницька парадигма національної безпеки виключає з процесів формування стратегій кіберпростору усі сектори, крім військового, економічна парадигма наголошує на важливості участі інших секторів та відомств у процесі формування стратегій кібербезпеки. Економічна парадигма наголошує на децентралізованому підході в групах відомств та суб’єктів, відповідальних за управління кібербезпекою. Згідно з цим підходом тягар вжиття заходів щодо захисту систем розподіляється між окремими особами, надавачами послуг (провайдерами) та керівництвом держави.

У третьому розділі – «Практичні аспекти забезпечення кібербезпеки у публічному секторі» – розглядаються практичні аспекти забезпечення кібербезпеки у публічному секторі, обґрунтовується необхідність формування глобального підходу до забезпечення кібербезпеки.

Встановлено, що інтеграція цифрового світу в повсякденне життя громадян привела до збільшення їх попиту як користувачів на прозорість публічного управління, доступ до інформації та її доступність, а також на можливість отримання зворотного зв’язку з органами влади та іншими публічними організаціями. Органи влади багатьох країн за останні десять років стали активними учасниками так званого «цифрового руху», який згодом назвали «уряд 2.0» або просто «Gov 2.0», у якому важливе місце посідають соціальні мережі. При цьому одним з ключових питань політики кібербезпеки, що стоять перед публічними чиновниками при розгляді рішень про те, як краще за все впровадити соціальні мережі в діяльність публічних організацій, є питання забезпечення належного балансу між управлінням ризиками і створенням дійсно відкритого уряду. Це не дивно, оскільки існує природне протиріччя між характеристиками відкритого уряду, – відкритими даними, відкритим доступом, прозорістю і підзвітністю, – і проблемами забезпечення

безпеки.

З’ясовано, що особливо в соціальних мережах найбільш реальною загрозою безпеки може бути ненавмисне розкриття потенційно компрометуючої інформації або непублічних даних недбалими публічними службовцями. У той же час, більша частина привабливості соціальних мереж полягає в їх здатності «пов’язувати» велику кількість людей в режимі реального часу. Тому в режимі реального часу Gov 2.0 надає великі можливості, в тому числі можливість інформувати учасників про різні деталі по мірі того, як відбуваються події, і надавати відкриті канали, які можуть негайно з’єднати різних акторів. Однак взаємодія в реальному часі також може не давати достатньо часу і концентрації зусиль для надання правильних відповідей, і збільшує ймовірність того, що публічні службовці можуть надати інформацію, яка ще не була перевірена, відповідно, може завдати шкоди безпеці. Крім того, експонентне щоденне зростання соціальних мереж, сервісів і додатків надає численні нові потенційні точки входу в комп’ютерні мережі. Це одна з найбільш основних і очевидних загроз, яку не можна ігнорувати.

Визначено, що правові, технічні та процедурні заходи й організаційні структури щодо забезпечення кібербезпеки повинні бути зроблені / створені на національному рівні, а також узгоджені на міжнародному рівні в такий спосіб: національні закони повинні прийматися там, де їх ще немає, а існуючі закони, а також регіональні та міжнародні угоди повинні ґрунтуватися на загальному розумінні того, що являють собою загрози кібербезпеки; технічні рішення повинні бути визначені та розроблені з урахуванням загальноприйнятих стандартів, спрямованих на забезпечення базових показників безпеки апаратного та програмного забезпечення, які можуть бути прийняті виробниками, постачальниками і кінцевими користувачами; необхідно на національному рівні створити відповідні організаційні структури, такі як центри та групи координації та реагування (наприклад, групи реагування на комп’ютерні інциденти), щоб швидко реагувати на кібератаки і координувати дії зі своїми колегами на міжнародному рівні.

При аналізі діяльності міжнародних організацій у сфері кібербезпеки, було визначено декілька важливих напрямків дій, які повинні бути реалізовані в Україні для підвищення національної кібербезпеки в цілому і публічного сектора зокрема, а саме: 1) гармонізація національного законодавства в сфері кібербезпеки із законодавством ЄС; 2) впровадження стандартів і рекомендацій, розроблених МСЕ, які стосуються технічних аспектів забезпечення кібербезпеки; 3) створення на національному та регіональних рівнях спеціальних організаційних структур і команд протидії кіберзагрозам різного характеру; 4) реалізація масових освітніх програм, спрямованих на формування безпечної поведінки в кіберпросторі; 5) розширення міжнародного співробітництва в сфері кібербезпеки, участь в реалізації різних ініціатив у цій сфері. Також було визначено низку загальних аспектів, які повинні бути присутніми в політиці та стратегії кібербезпеки в Україні. До таких аспектів слід віднести: посилення координації органів влади на політичному та оперативному рівнях; зміцнення публічно-приватного співробітництва;

покращення міжнародного співробітництва; повага до фундаментальних цінностей; урахування питань суверенітету при розробці політики в сфері кібербезпеки; гнучкий підхід до формування та реалізації політики; важливість економічних аспектів кібербезпеки; важливість діалогу за участю багатьох зацікавлених сторін.

Визначено, що стратегії кібербезпеки відображають в стратегічних документах (таких як стратегія національної безпеки і стратегія кібербезпеки) процеси визначення кіберпростору як сфери, що потребує реалізації відповідних заходів безпеки. Відповідно до цього існує два основні підходи до реалізації державної політики щодо боротьби з кіберзагрозами: державницький та економічний (табл. 1). Доведено, що в Україні доцільно використовувати синтетичний підхід, який поєднує обидва зазначені підходи.

Таблиця 3.1.

Порівняння особливостей застосування державницького та економічного підходів в процесі реалізації державної політики щодо боротьби з кіберзагрозами

№	*Підходи*	*Економічний підхід*	*Державницький підхід*
1	Сприйняття кіберзагроз	Приватна безпека, інформаційно-комунікаційні технології (ІКТ)	Критична інфраструктура, ІКТ
2	Джерела кіберзагроз	Злочинці, недержавні суб'єкти, кіберзлочинці, хакери	Іноземні держави, шантажисти, терористи
3	Відомства, відповідальні за управління кібербезпекою	Міністерства внутрішніх справ, цивільні відомства та ін.	Міністерства оборони, інші військові відомства

З огляду на сучасну спрямованість на багатосуб'єктність у забезпеченні кібербезпеки, яка передбачає співпрацю публічного, приватного і третього секторів, було сформульовано ряд пропозицій для підвищення ефективності стратегій і політики кібербезпеки, а саме: 1) спільна систематична оцінка відповідності заходів кібербезпеки, пропонованих органами влади, іншим ініціативам у сфері кібербезпеки. Наприклад, законодавство, яке встановлює кримінальну відповідальність за хакерство, могло б взяти до уваги, що деякі дослідження сприяють підвищенню кібербезпеки, використовуючи такі ж методи, як і хакери; 2) публічні організації як власники і оператори інформаційних систем і мереж можуть подавати приклад іншим акторам, застосовуючи передовий досвід, технології і навіть законодавчі вимоги. Технології, розроблені для одного із секторів, також можуть принести користь іншим секторам; 3) політики можуть звернутися за порадою до технічного

товариства Інтернету якомога раніше в процесі розробки політики, щоб уникнути прийняття технологічно помилкових рішень; 4) політика в сфері кібербезпеки може стимулювати розробку відкритих стандартів, що дозволяють впроваджувати інновації для рішень у даній сфері, спираючись на шанованих в експертному співтоваристві і таких, що добре зарекомендували себе, фахівців зі стандартизації Інтернету, уникаючи при цьому односторонньої зміни стандартів Інтернету; 5) слід заохочувати збір емпіричних даних, щоб краще оцінювати актуальність стратегій і політик, а також підтримувати підходи, засновані на оцінці ризиків. Для протидії існуючим перешкодам, з якими багато акторів стикаються при наданні додаткової інформації про кіберінциденти, слід виділяти додаткові ресурси і впроваджувати узгоджені механізми повідомлення про порушення безпеки, з якими стикаються представники всіх трьох секторів.

Доведено, що політика кібербезпеки в Україні повинна ґрунтуватися на таких принципах: впровадження стратегічного підходу до забезпечення кібербезпеки; комплексне вирішення проблем кібербезпеки, включаючи використання ефективних механізмів координації, адаптованих до культури і стилю управління в країні; своєчасність, гнучкість і адаптивність у прийнятті рішень у сфері забезпечення кібербезпеки; розвиток національного потенціалу команд з протидії кіберінцидентам; впровадження передових методів забезпечення кібербезпеки; покращення захисту критично важливих інформаційних інфраструктур; повага до фундаментальних цінностей свободи інформації, але з використанням належних запобіжних заходів, стримувань і противаг; підвищення кіберграмотності суспільства; використання системи стимулів для розвитку сфери кібербезпеки і відповідного кадрового потенціалу; співпраця з приватними та неурядовими організаціями, розвиток публічно-приватного партнерства; посилення боротьби з кіберзлочинністю; заохочення досліджень і розробок у сфері кібербезпеки; розвиток міжнародного співробітництва, зокрема, шляхом участі в розробці загальних норм поведінки в кіберпросторі.

У четвертому розділі – «Запобігання та протидія кіберзагрозам в публічному секторі України: соціологічний аналіз» – аналізується сучасний стан і проблеми запобігання та протидії кіберзагрозам у публічному секторі України.

Результати проведеного соціологічного дослідження показали, що, на думку респондентів, рівень цифровізації та інформатизації, а відповідно і розвитку електронного урядування в Україні є невисоким (рис. 2). Двома основними причинами цього є такі: незадовільне матеріально-технічне забезпечення органів публічного управління, зокрема, застарілість комп‘ютерної та організаційної техніки тощо; відсутність швидкісного інтернету, особливо в невеличких містах, селищах і селах.

Виявлено, що головними кіберзагрозами для сучасної України є: крадіжка інформації, фінансове шахрайство і хакерські атаки. При цьому держава в цілому і органи публічного управління, зокрема, не є готовими сьогодні до адекватного реагування на ці загрози.

Рівень кіберзахисту у «публічному секторі» значно поступається

приватному. Державний сектор взагалі виявився найбільш незахищеним з точки зору протистояння кібератакам та витоку даних в Україні. Це зумовлено як недостатньою захищеністю інформаційних мереж, недосконалістю існуючого обладнання і програмного забезпечення, так і відсутністю кваліфікованих фахівців в сфері кіберзахисту. Виходячи з цього, держава не виступає суб'єктом, якому громадяни довіряють в питаннях кіберзахисту та захисту персональної інформації, зокрема. У даному разі більшість опитаних покладається на себе. При цьому найбільш захищеними від кібератак та витоку даних є IT-компанії та банківський сектор.

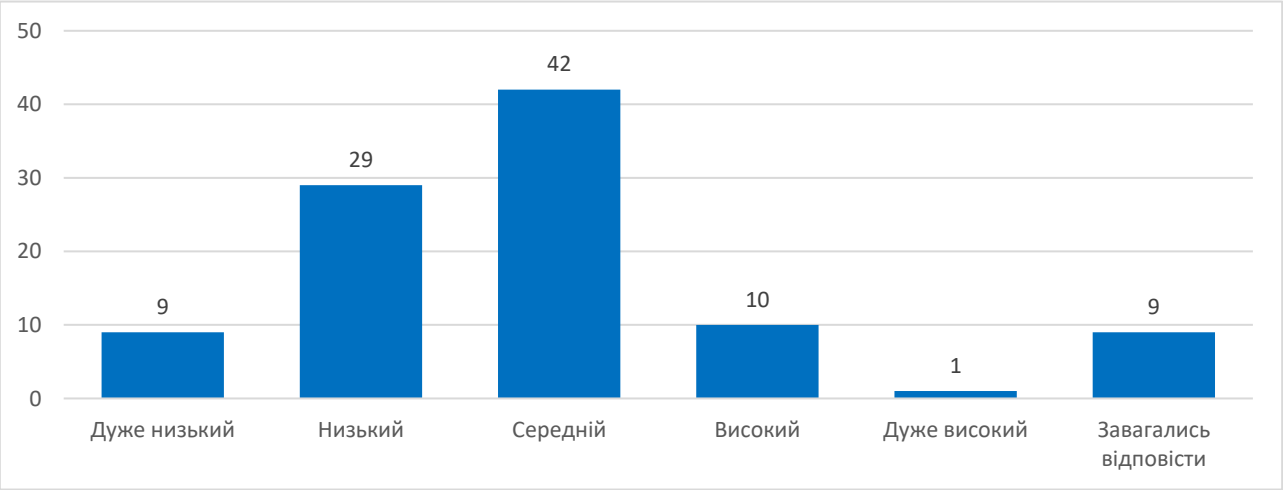

Рис. 2. Оцінка рівня розвитку електронного урядування в Україні (у % до всіх опитаних)

З'ясовано, що публічний сектор має сьогодні неабиякі проблеми з фінансуванням сфери кібербезпеки і в цьому питанні значно поступається приватному. Це зумовлено як недосконалістю державної політики у цій сфері (недостатня увага до цих проблем, низький рівень фінансування, відсутність ефективного моніторингу, тестувань, спеціальних підрозділів тощо), так і високою вартістю відповідного обладнання і програм.

Дослідження також довело низький рівень кваліфікації працівників органів публічного управління щодо кіберпитань в цілому та використання технологій організаційного і особистого кіберзахисту зокрема (рис. 3).

При цьому сама особиста недбалість та непідготовленість працівників визнається одним з найголовніших чинників успішних кібератак в публічному секторі. Спільною для всіх осіб, які працюють в органах публічного управління, є також потреба в опануванні технологій електронного документообігу та он-лайн комунікацій, що пов'язано із специфікою їх роботи.

З'ясовано, що основними шляхами підвищення рівня кібербезпеки в публічному секторі є, на думку респондентів, установка сучасного програмного забезпечення та його постійне оновлення, регулярне підвищення кваліфікації всіх працівників з питань захисту організаційної та персональної інформації,

створення власного підрозділу щодо захисту інформаційних ресурсів (рис. 4).

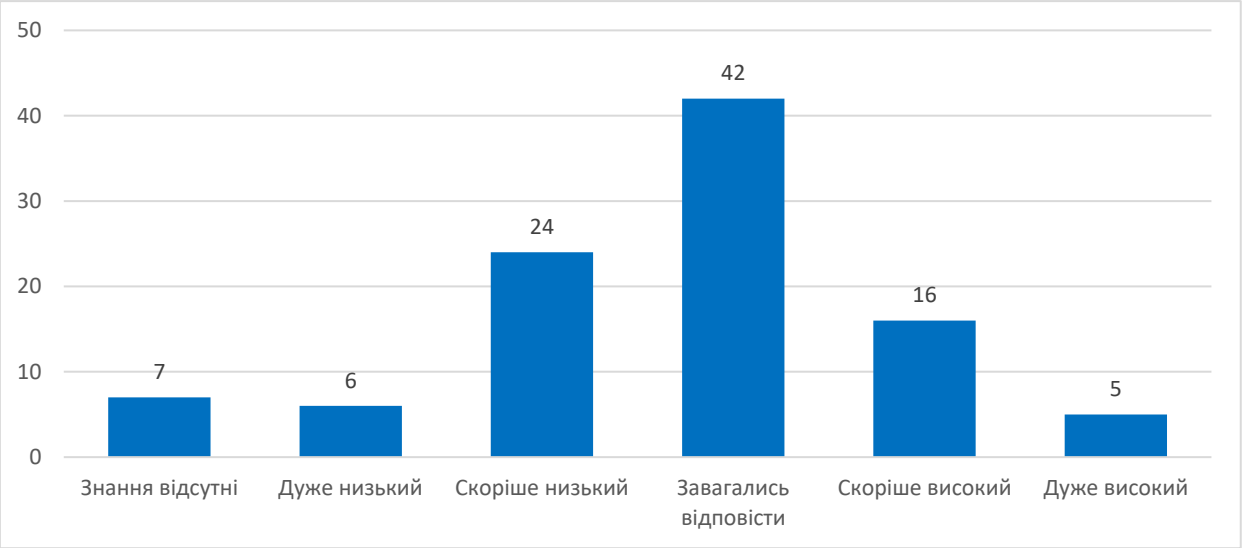

Рис. 3. Розподіл відповідей опитаних на запитання: «Яким є рівень Ваших знань, вмінь та навичок щодо захисту інформації Вашої організації від кіберзагроз»

Говорячи про пріоритетні напрями щодо інвестування (фінансування) для підвищення рівня кібербезпеки в країні в цілому, респонденти звернули увагу, насамперед, на кібераналітику (69%) і хмарні технології (50%). У публічному секторі важливими було визнано інвестування в хмарні технології і машинне навчання (по 52% відповідно). На рівні окремих організацій – в кібераналітику (66%) і хмарні технології (63%).

У п'ятому розділі – «Удосконалення забезпечення кібербезпеки в публічному секторі в сучасних умовах» – викладено пропозиції автора щодо удосконалення забезпечення кібербезпеки в публічному секторі.

З'ясовано, що у кіберсередовищі існують певні кіберризики. Кіберризик, який за своєю суттю існує у всіх IT-активах, є різновидом ризику, який виникає у різних акторів, від приватних осіб до міжнародних організацій, які мають критично важливі IT-активи. Кіберризик відрізняється від «звичайного» не лише одним конкретним ризиком, а й технологією, переносниками, засобами тощо. Більше того, кіберризики мають дві характеристики: великий потенційний вплив та низьку ймовірність.

Як показала практика останніх двадцяти років, можна визначити такий основний перелік кібератак: атаки соціальної інженерії в Інтернеті; мережеві сніфери та спуфінги пакетів; знаходження та використання вразливостей у програмному забезпеченні без вихідного коду; кіберзагрози та кібербулінг; автоматизовані зонди та скани; інструменти вторгнення графічного інтерфейсу; DDOS-атаки; промислове шпигунство; атаки на виконувані коди (проти браузерів); викрадення сесій; поширені атаки на інфраструктуру DNS та використання NNTP для розповсюдження атаки «Stealth» та інших

вдосконалених методів сканування; трояни віддаленого доступу на базі Windows (Back Orifice); поширення шкідливого коду електронною поштою; широкомасштабне розповсюдження троянів; атака на конкретних користувачів; широкомасштабне використання хробаків; складні атаки ботнет-команд; експлойти мобільних пристроїв на Android; Advance Persistent Threat (APT); хмарні атаки; вбудовані шкідливі програми; шкідливі компоненти на базі апаратного забезпечення; шкідливі програми Old School (MiniDuke).

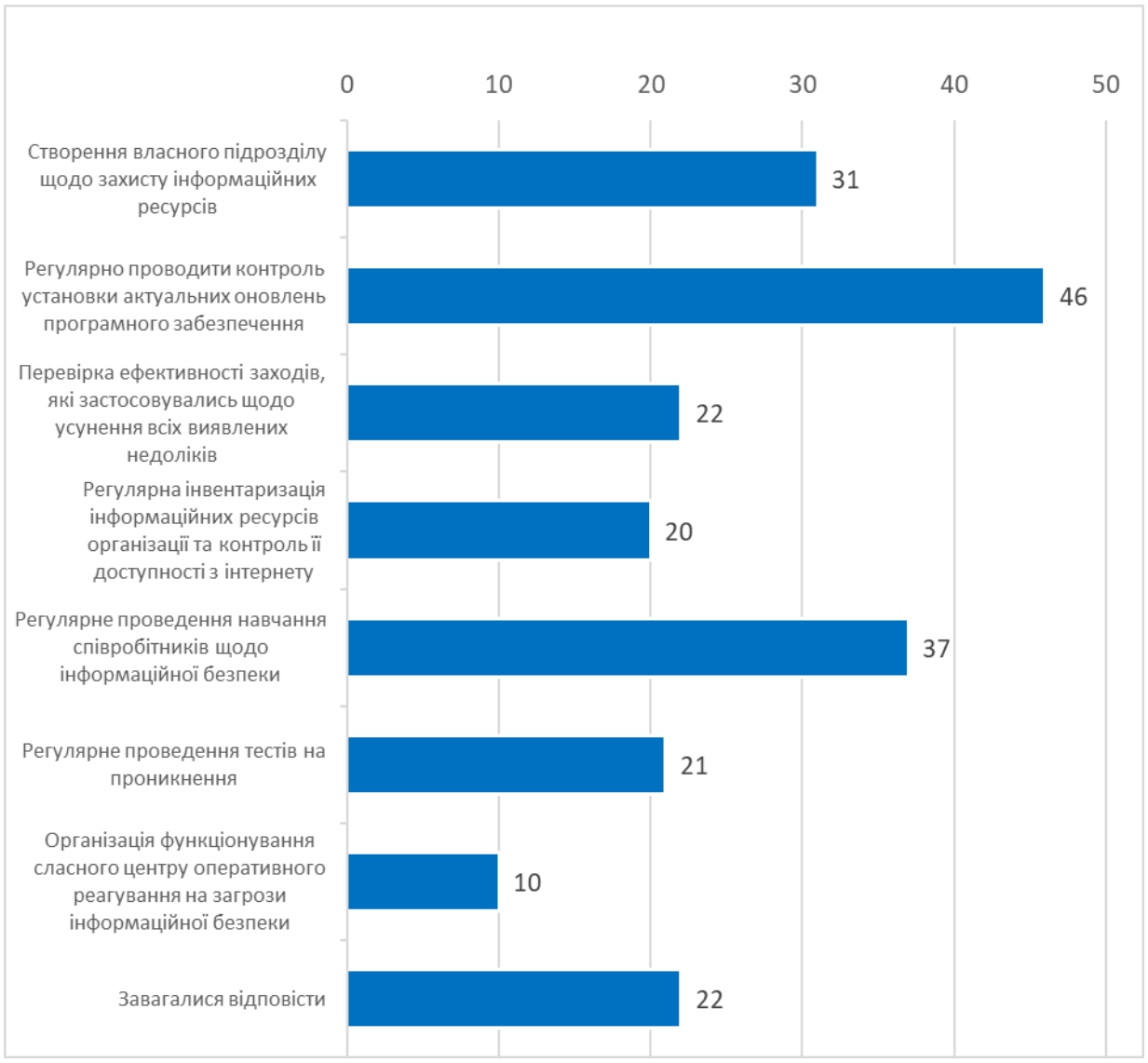

Рис. 4. Розподіл відповідей працівників органів публічного управління на запитання щодо заходів, які повинна вживати їх організація для підвищення рівня кібербезпеки (у % до всіх опитаних)

Визначено, що з урахуванням нових кіберризиків та більш складних шкідливих програм, країни та міжнародні організації, такі як НАТО, ENISA тощо, шукають нових способів боротьби зі складними проблемами у галузі кібербезпеки. Суттєвим кроком для країн є формування національної стратегії кібербезпеки та відповідних політик. Проте незважаючи на те, що ці стратегії та

політики інтенсивно охоплюють військову, розвідувальну та критичну інфраструктури, кібербезпека на рівні організацій часто ігнорується. Доведено, що для забезпечення надійної кібербезпеки на національному рівні має бути забезпечена кібербезпка і на рівні організацій.

Виходячи з цього було запропоновано модель інституційної кібербезпеки, яка включає увесь спектр акторів (приватні особи, публічні та приватні установи, національні безпекові структури та міжнародні організації). У запропонованій моделі організаційні актори розглядаються як основні, такі, що разом утворюють основу організації кібербезпеки. І хоча найслабшою ланкою в інформаційній безпеці вважається людина, з точки зору національної безпеки найслабшою ланкою є найслабша організація, що підлягає впливам кіберризиків. Але на відміну від зазначених у національних стратегіях кібербезпеки положеннях, з точки зору моделі інституційної кібербезпеки, для забезпечення надійної кібербезпеки слід брати до уваги не лише організації, які управляють критичною інфраструктурою, а й всі інші організації, що мають кіберзахист.

Запропонована модель інституційної кібербезпеки (рис. 5) забезпечує загальний підхід, за допомогою якого кожна організація може адаптувати дану модель до власних потреб безпеки, для розвитку своїх можливостей із забезпечення кібербезпеки.

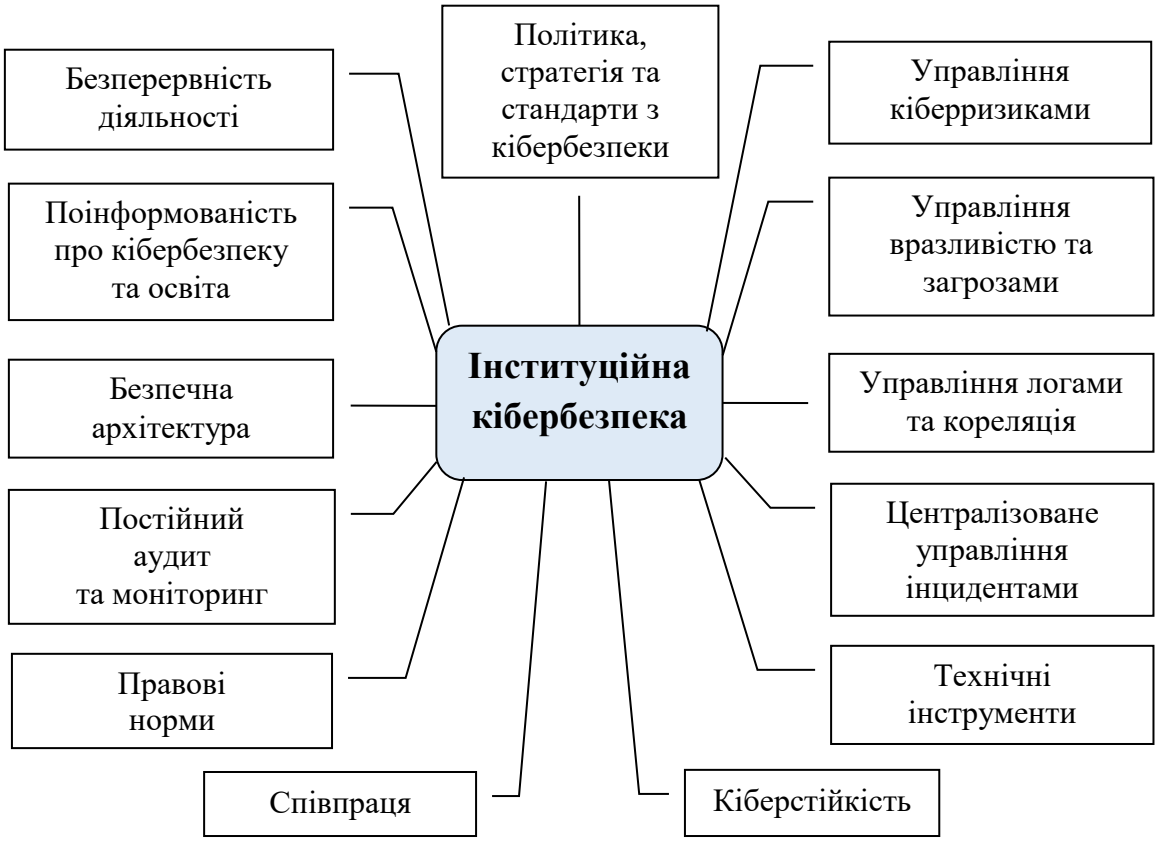

Рис. 4. Модель інституційної кібербезпеки

Для досягнення цієї мети було визначено основні принципи інституційної кібербезпеки, що випливають з моделі: підхід до кібербезпеки повинен бути холістичним; слід застосовувати гнучкий стиль управління; слід впроваджувати методи постійного вдосконалення діяльності, орієнтовані на управління ризиками; на додаток до координації діяльності публічних, приватних, академічних та неурядових організацій; міжнародна співпраця та обмін інформацією також мають складати базис забезпечення кібербезпеки; мають заохочуватись прозорість, підзвітність, етичні цінності, свобода слова; важливим є встановлення балансу між безпекою та застосовністю ІТ-продуктів і технологій.

Обґрунтовано інтегровану теоретико-методологічну модель розробки національної стратегії кібербезпеки (рис. 6), відповідно до якої актори у кіберпросторі (державні актори, недержавні актори, кінцеві користувачі та кіберзлочинці) здійснюють дії (проводять політику, слідують політиці, атакують, захищаються від нападів, отримують і передають інформацію, здійснюють комунікацію, використовують ІКТ для роботи й у побуті тощо), які перетинаються з різними аспектами кіберпростору та кібербезпеки (політичними, соціальними, культурними, технологічними) та породжують явища кібербезпеки, такі як вразливості, цілісність системи, шкідлива поведінка, ідентичність, мотивація тощо.

Визначено, що державні та недержавні актори, конкуренція за відносні вигоди та політичні аспекти кібербезпеки вимагають неореалістичного підходу до її забезпечення і формулювання відповідних положень стратегії кібербезпеки. У той же час, інтерсекційність дозволяє врахувати у стратегії кібербезпеки соціальні аспекти, зокрема, такі як рівність і справедливість у кіберпросторі, адже ці фактори часто становлять причини злочинної групової поведінки у кіберсередовищі. Кінцеві користувачі, кіберзлочинці та їх поведінка є продуктом їхньої ідентичності як представників певного національного культурного середовища, так і користувачів Інтернет. Врахувати культурні аспекти кібербезпеки допоможе соціальний конструктивізм. Нарешті, кібервестфалізм дозволяє врахувати у стратегії кібербезпеки сучасні технологічні аспекти та їхній вплив на інші аспекти кіберпростору та кібербезпеки.

Встановлено, що зі стратегічної точки зору кібербезпека реагує на захист національних інтересів та активно реалізує ці інтереси, а кіберпростір сприймається як середовище загроз та можливостей, в якому держава повинна діяти задля власного збереження та досягнення власних цілей. Крім того, кіберпростір проблематизується як місце і як джерело небезпеки. Відповідно, кіберпростір можна розглядати як суму двох компонентів. Перший – це фізичний субстрат кіберпростору: комп’ютери та мережі, в які вони зібрані та через які вони «спілкуються». Другий – це комунікації, яким сприяє цей фізичний рівень: мережева, цифрова діяльність, що включає вміст і дії, які здійснюються через цифрові мережі. Обмін інформацією залежить від існування фізичного рівня, який апріорі необхідний для існування кіберпростору. Кіберпростір є як фактичним, так і віртуальним, у тому сенсі,

що кіберпростір є частково віртуальним середовищем, що ґрунтується на суттєвості фізичних систем. Інформація, якою обмінюються та на яку реагують, може бути далі розмежована на синтаксичний та семантичний рівень. Синтаксичний рівень – це місце, де комп'ютери взаємодіють між собою, і містить домовленості, за якими вони це роблять, такі як протоколи TCP / IP, які керують маршрутизацією інтернет-трафіку. Семантичний рівень – це той, де інформація створюється, зберігається та маніпулюється акторами для соціальних, економічних та політичних цілей. В основному саме цей семантичний рівень можна назвати цифровою діяльністю.

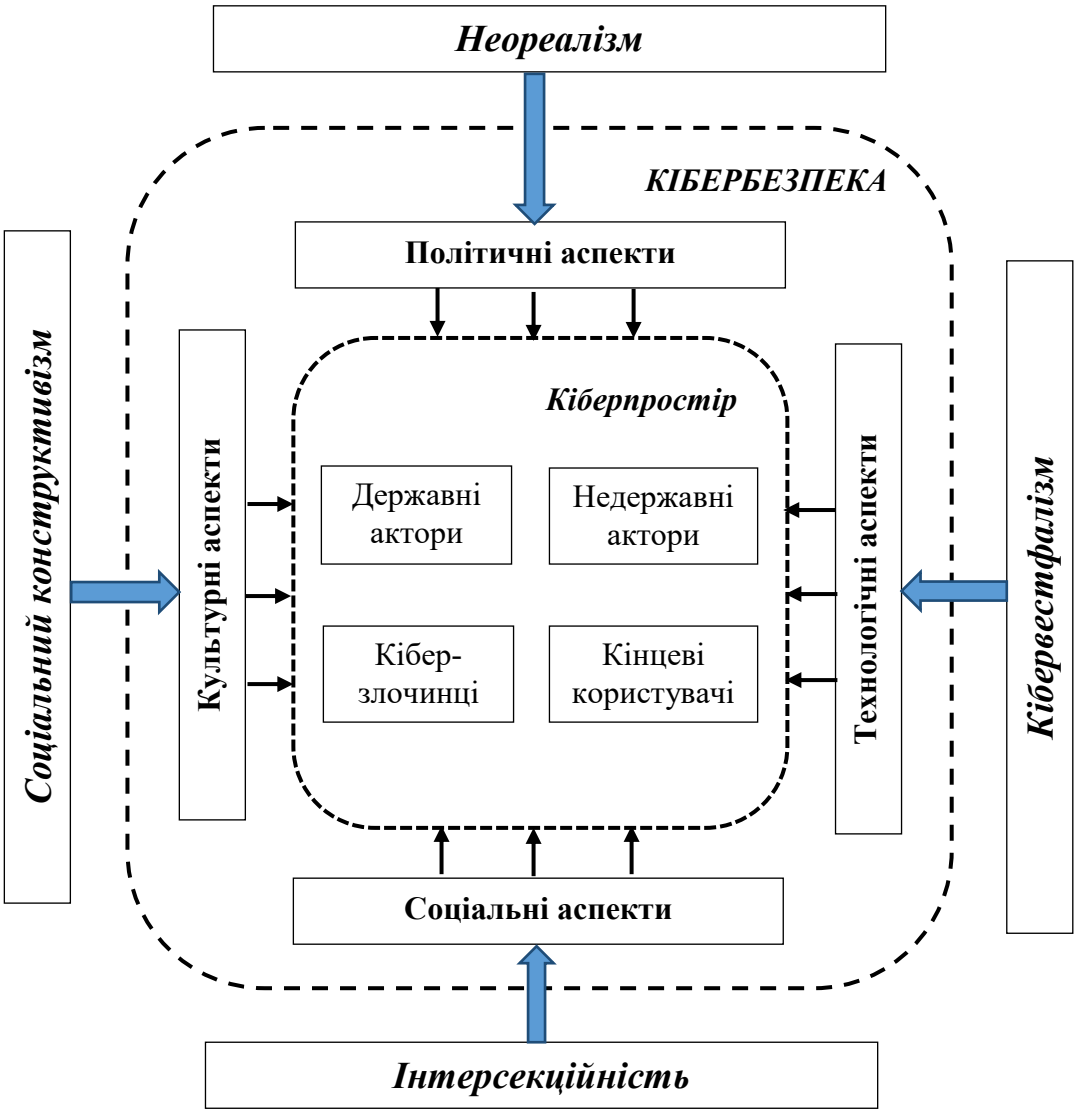

Рис. 6. Теоретико-методологічна модель розробки національної стратегії кібербезпеки

Отже, кіберпростір є середовищем як технологічної, так і соціальної дії, хоча сам по собі не є інфраструктурою. Тому безпека кіберпростору (кібербезпека) повинна функціонувати як у технологічному, так і в соціальному вимірах. Таким чином, як стратегічна сфера, кіберпростір також повинен бути доменом влади. «Домен» слід розуміти як у просторовому розумінні –

кіберпростір настільки фізичний, скільки і віртуальний, але також і у вужчому розумінні – як колективність соціальних суб'єктів, які зазнають впливу певної форми влади.

Визначено, що публічно-приватне партнерство (ППП) у сфері кібербезпеки актуалізує три важливі питання. Перше питання – це питання вимірювання ефективності партнерства для того, щоб однозначно з'ясувати, чи демонструють члени ППП взаємно вдосконалений кіберзахист в результаті своїх партнерських відносин. Впровадження системи показників ефективності може бути корисним як публічним, так і приватним партнерам, оскільки може заохотити додаткову участь та визначити сфери партнерства, які потребують вдосконалення. Для публічного сектора показники можуть бути зосереджені на показниках участі в галузі, кількості унікальних шкідливих підписів, внесених групами-членами, або на деякий розрахунок часу та ресурсів, що витрачаються на виконання завдань партнерства, таких як зустрічі чи розповсюдження інформації.

Друге питання – це питання зобов'язань. Майже всі дослідження з ППП, у тому числі, у сфері кіберзахисту, показують, що існують проблеми між державними та приватними членами цих партнерств через мотиваційні чинники. У цілому, публічний сектор мотивується прагненням забезпечення національної оборони та національної безпеки, а приватний сектор мотивується фінансовими аспектами – або витратами, або доходами. Ці спонукання проникають в інші аспекти відносин і можуть негативно впливати на партнерство, особливо, якщо існує ситуація «перебільшених очікувань». Для того, щоб це не відбувалось має бути встановлений і прийнятий всіма членами партнерства чіткий розподіл зобов'язань кожного члена, причому до реального початку партнерства.

Третє питання – це питання стримування. Відповідні дослідження чітко показують, що довіра є наріжним каменем, головною складовою партнерських відносин. Довіра впливає на участь, на внески членів та на те, як вони взагалі сприймають цінність цих партнерських відносин. Саме з довіри чи її відсутності випливає питання того, що ми зазначили як «стримування». Саме відсутність повної довіри призводить до того, що члени партнерства «стримуються» у відносинах один з одним. Вони стримують результати тестів на проникнення, які можуть визначити, як зловмисники отримали доступ, бо бояться впливу на свій імідж. Вони стримують обмін інформацією, щоб не дати конкурентам уявлення про свою незахищеність. Вони стримують надання даних про тактику, прийоми та процедури фінансованих державою кіберкампаній через страх висвітлення своєї діяльності. Вони стримують фінансування для розробки або придбання ефективних систем попередження, які можуть миттєво обмінюватися даними про загрози, виявляти вразливі місця та надавати програмні виправлення. Вони стримують навчання своїх працівників щодо розуміння кіберзагроз, розуміння того, як поведінка користувачів забезпечує віктимізацію, або як донести цю проблему до керівництва. Вони стримуються, висуваючи чіткі цілі та очікування щодо цих відносин. Але в основному вони стримують свою чесність щодо того, що

насправді працює, а що не працює. І існує єдиний шлях подолання всього цього стримування – це встановлення дійсно довірчих відносин у партнерстві.

ВИСНОВКИ

У дисертації вирішено актуальну наукову проблему щодо розробки теоретико-методологічних засад забезпечення кібербезпеки в публічному секторі в сучасних умовах. Отримані в процесі дослідження результати свідчать про реалізацію поставлених мети й завдань і дають можливість зробити такі основні висновки:

1. Визначено, що кібербезпека охоплює широкий набір практик: оцінка ризиків і тестування проникнення; аварійне відновлення; криптографія; контроль та спостереження за доступом; мережева архітектура, програмне забезпечення та безпека; безпекові операції; фізична безпека тощо. При цьому кібербезпека має три основні складові: 1) інформаційно-комунікаційні системи, які є надійними і можуть протистояти атакам; 2) методи та системи виявлення загрози та аномалій для забезпечення стійкості інформаційно-комунікаційних систем; 3) забезпечення системної реактивності на кібератаки. Встановлено, що впровадження систем кібербезпеки має важливі наслідки для публічних інтересів інформаційного суспільства, оскільки це дає можливість належного функціонування критично важливих національних інфраструктур, і дозволяє громадянам здійснювати свою рутинну діяльність, спираючись на безпечні технології. Виходячи з цього, кібербезпеку слід розглядати як суспільне благо. Було зазначено, що три важливі переваги випливають із управління кібербезпекою як суспільним благом: системний підхід до безпеки, спільна відповідальність між різними стейкхолдерами, розвиток співпраці у сфері кібербезпеки.

2. З’ясовано, що поняття кібербезпеки у цілому та в публічному секторі зокрема безпосередньо пов’язане з феноменом інформаційного суспільства та електронного врядування, що з’явилось внаслідок розвитку інформаційного суспільства. Електронне врядування ґрунтується на трьох «стовпах»: довірі, прозорості та підзвітності, які є нерозривно взаємопов’язаними. З іншого боку, на сучасний світ у цілому та публічне управління зокрема впливають процеси глобалізації. Виходячи з цього, а також враховуючи особливості публічного сектора, для нього було визначено п’ять основних викликів щодо забезпечення кібербезпеки: 1) публічному сектору властива велика ступінь оперативної незалежності та «ізольованості» між різними його частинами, що робить для нього вирішення питань кібербезпеки набагато більш складним ніж для приватного; 2) важливі загальнодоступні дані створюються, зберігаються та застосовуються відповідними суб’єктами поза органами публічної влади, тому визначення безпеки публічного сектора має бути розширеним та переосмисленим; 3) поведінка людини, раціональна або нераціональна, є стрижнем кібербезпеки, тому необхідними є заходи для формування безпечної поведінки у кіберпросторі; 4) існує зворотна залежність між використанням інформаційно-комунікаційних технологій і кібербезпекою, тому необхідним є

забезпечення тут певної рівноваги; 5) користувачі електронного уряду потребують такого ж кіберзахисту від органів публічної влади, як органи публічної влади потребують захисту від третьої сторони, тому важливим є налагодження партнерства щодо забезпечення кібербезпеки.

3. Встановлено, що концептуальні засади забезпечення кібербезпеки в органах публічної влади складають, з одного боку, виміри кібербезпеки (людський, організаційний, інфраструктурний, технологічний, нормативний), з іншого боку – дії, необхідні для забезпечення кібербезпеки. Людський вимір є найбільш фундаментальним і, у той же час, найбільш слабким елементом кібербезпеки, оскільки хоча кіберпростір побудований на технологіях, людина управляє ними і контролює їх, а недостатня поінформованість і недостатні знання роблять людей найбільш вразливою ланкою в порівнянні з іншими. Організаційний вимір зосереджений на інститутах всередині кіберпростору, це функціональна структура, яка контролює кіберпростір, і зміцнення цього виміру може відбуватись за двома напрямами: 1) стратегічні дії орієнтовані всередині країни, такі як підвищення потенціалу і можливостей відповідної структури; 2) стратегічні дії орієнтовані назовні, які активізують співпрацю для забезпечення безпеки кіберпростору. Інфраструктурний вимір є середовищем, яке створює кіберпростір, без інфраструктури кіберпростір – ніщо, тому зміцнення цього виміру необхідно для підтримки кіберсередовища у цілому; якщо цей вимір слабкий, транзакції в кіберпросторі можуть «впасти». Технологічний вимір розширює можливості кіберпростору, і оскільки кіберпростір включає в себе найбільш передові технології, зміцнення цього виміру означає впровадження новітніх та найбільш ефективних технологій, що забезпечують кібербезпеку і дозволяють проводити подальші дослідження і розробки у цій сфері. Нормативний вимір структурує кібербезпеку і створює певне імперативне середовище у кіберпросторі, цей вимір спрямований на формування національної кібер-екосистеми шляхом створення і застосування нормативно-правової бази та розробки необхідних стандартів.

4. Узагальнення зарубіжних практик щодо забезпечення кібербезпеки у публічному секторі показало, що кожна з розглянутих країн має власні національні стратегії кібербезпеки (НСК) і відповідне законодавство для вирішення проблем кібербезпеки. В більшості НСК загрози для критичної інфраструктури та кіберзлочинність відіграють важливу роль і вказують на зростання шкоди для економіки, завданої кібератаками. У формальному сенсі, сфера кіберпростору вже включена до порядку денного з питань безпеки всіх держав, однак у підходах до її забезпечення є відмінності. Забезпечення кібербезпеки відрізняється за тим, як держави, по-перше, визначають референтний об’єкт (що потрібно захищати), по-друге, сприймають основні загрози та ризики та, по-третє, визначають джерела загроз та ризики. Відповідно до цих відмінностей їх можна віднести до двох категорій. Перша категорія – держави, що мілітаризують питання кібербезпеки. Ці держави більш точно визначають конкретні референтні об’єкти та називають захист цих об’єктів національним пріоритетом. Такий підхід піднімає кібербезпеку на найвищий рівень національної безпеки та зосереджує увагу на захисті ІКТ та

державних інформаційних ресурсів. Відповідно, відповідальність за реагування на кіберзагрози у цих державах передана воєнним та оборонним органам. Друга категорія – держави, що криміналізують питання кібербезпеки, покладаючись на економічний підхід у забезпеченні кібербезпеки. Їхні референтні об'єкти відрізняються і здебільшого стосуються належного функціонування системи національної економіки та приватної власності. ІКТ та державні цифрові ресурси не мають переваги над іншими законними референтними об'єктами. Унаслідок цього держави з домінуючим економічним підходом зосереджуються на кримінальній діяльності у кіберпросторі, а проблеми кібербезпеки розглядають як «ризики». Перелік потенційних джерел таких ризиків також фрагментований і включає не лише зовнішні міжнародні суб'єкти, але також внутрішні суб'єкти – хакерів, хактивістів, кримінальні організації і навіть ненавмисні злами мереж. На нашу думку, в Україні доцільно використовувати обидва зазначені підходи разом, оскільки це сприятиме кращому розумінню кібербезпеки як явища і допоможе пояснити перешкоди для співпраці держав, що займаються питаннями кібербезпеки на міжнародному рівні. Крім того, визначення особливостей різних підходів до кібербезпеки може пояснити конкретні дії держав у кіберпросторі. Розуміння відмінностей в сприйнятті державами кіберзагроз, референтних об'єктів і потенційних противників становить основу для обговорення так званої кіберідентичності держав та недержавних суб'єктів. Це може бути корисним теоретичним знаряддям для аналізу потенційних кіберконфліктів та моделей співпраці у цій сфері.

5. Встановлено, що за останній час загрози кібербезпеці в публічному секторі постійно зростають і стають більш складними, і певним чином це пов'язано із впровадженням соціальних мереж і Gov 2.0 у діяльність публічних організацій, які намагаються стати більш відкритими і прозорими. Однак, незважаючи на загрози, органи влади на всіх рівнях, і особливо місцеві органи влади, повинні продовжувати впроваджувати і сприяти розробці нових технологій і рішень Gov 2.0, щоб залишатися надійними постачальниками публічних послуг та інформації. Тим не менше, органи влади повинні робити це обережно, стратегічно, маючи відповідну політику, розробляючи необхідні керівні принципи, використовуючи відповідні технологічні інструменти та навчання персоналу для захисту від загроз кібербезпеки. Наявність відповідної політики та керівних принципів у сфері кібербезпеки також є позитивним сигналом для громадян, нагадуючи про основоположну природу Gov 2.0 як про рух до відкритої, прозорої та безпечної арени діяльності публічних організацій. Громадяни в світі Web 2.0 очікують інтеграції таких технологій в свої взаємодії з публічними структурами, але як і раніше існують основні проблеми конфіденційності та обміну інформацією. Надання керівництв і політик може пом'якшити такі побоювання і відкрити для обговорення додаткові потреби і очікування громадян щодо ступеня розвитку сфери ІКТ. Публічні комунікації повинні мати свої власні керівні принципи, щоб гарантувати, що користувачі розуміють, куди направляється їх інформація, що очікується від її вмісту і яким чином цей вміст може бути видалено, показано або змінено. Рекомендації по

загальнодоступним комунікаціям допомагають сформувати очікування, полегшують діалог і зменшують потенційні проблеми, які можуть виникнути в результаті видалення / зміни контенту. Слід також визначити правила у відношенні того, яким чином інформація надається для публічного доступу. У цілому, було визначено, що забезпечення кібербезпеки у середовищі Gov 2.0 має ґрунтуватись на реалізації таких заходів: модерування контенту публічних аккаунтів; запобігання несанкціонованому використанню і передачі конфіденційної інформації; використання браузерів з обмеженими привілеями; впровадження систем виявлення / запобігання вторгнень; використання сервісів Web-репутації; фільтрація універсального локатора ресурсів (URL) та Інтернет-протоколу (IP); фільтрація шкідливих програм по периметру мережі; використання інструментів попереднього перегляду скорочення URL.

6. Визначено, що з урахуванням нових кіберризиків та більш складних шкідливих програм, країни та міжнародні організації, такі як НАТО, ENISA тощо, шукають нових способів боротьби зі складними проблемами у галузі кібербезпеки. Суттєвим кроком для країн є формування національної стратегії кібербезпеки та відповідних політик. Однак, незважаючи на те, що ці стратегії та політики інтенсивно охоплюють військову, розвідувальну та критичну інфраструктури, кібербезпека на рівні організацій часто ігнорується. Проте доведено, що для забезпечення надійної кібербезпеки на національному рівні має бути забезпечена кібербезпека і на рівні організацій. Виходячи з цього було запропоновано модель інституційної кібербезпеки, яка включає увесь спектр акторів (приватні особи, публічні та приватні установи, національні безпекові структури та міжнародні організації), та відповідно до якої інституційна кібербезпека повинна мати такі основні компоненти: політика, стратегія та стандарти з кібербезпеки; управління кіберризиками; управління вразливістю та загрозами; централізоване управління інцидентами; поінформованість про кібербезпеку та освіта; управління логами та кореляція; безпечна архітектура; правові норми; технічні інструменти; безперервність діяльності; постійний аудит та моніторинг; співпраця; кіберстійкість.

7. Доведено необхідність реалізації комплексу взаємопов’язаних заходів, спрямованих на підвищення рівня кібербезпеки в публічному секторі. Вони передбачають реалізацію: заходів організаційного характеру, зокрема, через утворення спеціальних підрозділів в штатному розписі органів публічної влади; заходів фінансового характеру, які передбачають обов‘язкове фінансування в державному та місцевому бюджетах коштів на кіберзахист, інвестування в кібераналітику і хмарні технології; кадрових заходів, що включають регулярне підвищення кваліфікації всіх державних службовців і посадових осіб органів місцевого самоврядування з питань захисту організаційної та персональної інформації, електронного документообігу, онлайн комунікацій тощо; заходів матеріально-технічного характеру, метою яких є постійне оновлення комп‘ютерного обладнання та його програмного забезпечення.

8. Показано, що запропонована модель інституційної кібербезпеки забезпечує загальний підхід, за допомогою якого кожна організація може

адаптувати дану модель до власних потреб безпеки для розвитку своїх можливостей із забезпечення кібербезпеки. Для досягнення цієї мети було визначено основні принципи інституційної кібербезпеки, що випливають із запропонованої моделі, і до яких належать такі: 1) підхід до кібербезпеки повинен бути холістичним; 2) слід застосувати гнучкий стиль управління; 3) слід впроваджувати методи постійного вдосконалення діяльності, орієнтовані на управління ризиками; 4) на додаток до координації діяльності публічних, приватних, академічних та неурядових організацій, міжнародна співпраця та обмін інформацією також мають складати базис забезпечення кібербезпеки; 5) у забезпеченні кібербезпеки мають заохочуватись прозорість, підзвітність, етичні цінності, свобода слова; 6) важливим є встановлення балансу між кібербезпекою та застосовністю ІТ-продуктів і технологій.

9. З'ясовано, що поступова, але послідовна мілітаризація та централізація управління посилюється в країнах, які є головними об'єктами кібератак, таких як США чи країни ЄС. Тому в цих країнах підходи до забезпечення кібербезпеки найбільше нагадують підходи неореалізму, з точки зору якого, фокус зосереджений на державах, а влада та безпека розглядаються як функції відносної вигоди від конкуруючих суперників. Однак, неореалізм не розпізнає загрози та можливості для більшої цілісності систем, які представляють недержавні актори та технології. Зробити це можна з позицій соціального конструктивізму, який вміє аналізувати спільне сприйняття як всередині, так і поза суспільством, і вміє розпізнавати як функцію ідентичності в динаміці національної безпеки, так і те, як ці сприйняття впливають на безпеку. Проте неореалістичний та соціально-конструктивістський підходи обидва розроблені як інтерпретації традиційної міжнародної безпеки, і по суті, жоден з них не включає інформаційні технології у свій дискурс. Уникнути цього недоліку дозволяє кібервестфаліанство, яке базується на розвитку можливих або ймовірних майбутніх технологій, і стверджує, що державна централізація Інтернету в багатьох країнах, спільно з розвитком цих майбутніх технологій, призведе до появи національних «кібермеж». Однак ця теорія не приділяє уваги ролі, яку відіграють чи можуть відігравати окремі громадяни, та їх поведінці у кіберпросторі. Кібервестфаліанство також дещо обмежене за своїм обсягом (кіберпростір) та підходом до рішень (технологія). Воно також не враховує економічну, політичну та військову динаміку між великими, середніми та регіональними державами. Усунути ці проблеми може певним чином теорія інтерсекційності, якщо її застосувати до кіберзбезпеки. Враховуючи зазначене було визначено, що теоретико-методологічна основа розробки національних стратегій кібербезпеки має ґрунтуватись на інтегративному підході, який містить елементи інтерсекційності, неореалізму, соціального конструктивізму та кібервестфаліанства.

10. Встановлено, що як стратегічна сфера, кіберпростір також повинен бути доменом влади. «Домен» слід розуміти як у просторовому розумінні – кіберпростір настільки фізичний, скільки і віртуальний, але також і у вужчому розумінні – як колективність соціальних суб'єктів, які зазнають впливу певної форми влади. З'ясовано при цьому, що в основі концепції влади є два «виміри».

Перший вимір – це види соціальних відносин, за допомогою яких впливає (та реалізується) спроможність суб'єктів, а другий вимір – специфіка цих соціальних відносин. Перший вимір відрізняється тим, як виражається влада: або через взаємодію між соціальними суб'єктами, або через регуляторні соціальні відносини. Другий вимір влади стосується специфіки соціальних відносин влади, будь то прямі та безпосередні, або опосередковані та дифузні. Зазначені два виміри разом створюють чотири типи влади: примусова, інституційна, структурна, продуктивна. Було доведено, що стосовно кібербезпеки примусова влада надає можливості для безпосереднього контролю одного актора з боку іншого; інституційна влада надає можливість опосередкованого контролю над акторами за посередництва інститутів; структурна влада визначає соціальні можливості та інтереси шляхом реалізації державно-приватних партнерських відносин; продуктивна влада дає можливість з'ясувати, яким чином системи знань та дискурсивні практики функціонують у мережах соціальних сил, породжених кібербезпекою.

11. З'ясовано, що на даний час поширюється створення середовищ, де публічний і приватний сектор активно та успішно співпрацюють – іноді як клієнт і постачальник, іноді через нагляд і дотримання, іноді як партнери. Ці домовленості зазвичай переслідують спільні цілі отримання певних позитивних результатів, але в деяких випадках партнерські відносини формуються як захисна відповідь спільним противникам. Саме така мета партнерства є головною у сфері забезпечення кібербезпеки. Публічно-приватне партнерство (ППП) як захисна модель покладається на те, що кожен учасник вносить щось унікальне в партнерство, що може пом'якшити його слабкі сторони та посилити його сильні сторони. Для ППП, орієнтованих на кібербезпеку, саме ступінь спільних наслідків пов'язує його учасників. Таке призначення зумовлює для публічного сектора необхідність визначити кібербезпеку приватних організацій як проблему національної безпеки, а отже, визнати відповідальність уряду за її забезпечення. Приватний сектор, у свою чергу, створює, управляє та підтримує системи, технології та процеси, що складають критичну інфраструктуру, забезпечення кібербезпеки якої є складовою забезпечення національної безпеки. Виходячи з цього і враховуючи наявні проблеми у даній сфері було обґрунтовано основні принципи публічно-приватного партнерства у сфері забезпечення кібербезпеки, а саме: перехід від «класичного» партнерства до взаємовигідної співпраці; визначення ролей членів партнерства за допомогою підходів управління ризиками; запровадження спільної відповідальності членів партнерства щодо загроз і вразливостей; впровадження системи оцінювання партнерства.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

монографічні видання:

1. Котух Є.В. Кібербезпека у публічному секторі : монографія / Є.В. Котух. – Харків : Колегіум, 2021. – 272 с.

в яких опубліковані основні наукові результати дисертації:

2. Котух Є.В. Особливості національної та регіональної політики у сфері кібербезпеки / Є.В. Котух // Теорія та практика державного управління. – 2019. – № 4(67). – С. 40-47.

3. Котух Є.В. Проблеми кібербезпеки в сучасному світі // Актуальні проблеми державного управління. – 2019. – №2(56). – С. 33-38.

4. Котух Є.В. Особливості забезпечення кібербезпеки в публічному секторі в умовах глобалізації / Є.В. Котух // Державне будівництво. – 2019. – № 2. – Режим доступу: http://db.journal.kharkiv.ua/index.php/db/article/view/65/60.

5. Котух Є.В. Формування систем кібербезпеки в органах публічної влади / Є.В. Котух // Державне управління: удосконалення та розвиток. – 2020. – № 3, березень. – Режим доступу: http://www.dy.nayka.com.ua/pdf/3_2020/32.pdf.

6. Котух Є.В. Електронне урядування як нова парадигма публічного управління / Є.В. Котух // Інвестиції: практика та досвід. – 2020. – № 3, лютий. – С. 122-127.

7. Котух Є.В. Електронний уряд і кібербезпека у соціальних мережах: особливості реалізації // Вісник НУЦЗ України. Серія: Державне управління. – 2020. – № 2. – С. 564-572.

8. Котух Є.В. Основні виклики врядування у сфері кібербезпеки / Є. Котух, В. Ободяк // Теорія та практика державного управління. – 2020. – № 4 (71). – С. 38-46.

Особистий внесок здобувача: визначено характеристики врядування у сфері кібербезпеки та ресурси кіберпростору.

9. Котух Є.В. Кібербезпека як один з пріоритетів національної політики / В.Б. Дзюндзюк, Є.В. Котух // Державне будівництво. – 2020. – № 2. – Режим доступу: http://db.journal.kharkiv.ua/index.php/db/article/download/90/85.

Особистий внесок здобувача: визначено пріоритетні напрями реалізації стратегій кібербезпеки.

10. Котух Є.В. Сучасний стан та проблеми «цифровізації» в Україні / Є.В. Котух, А.С. Довбиш // Актуальні проблеми державного управління. – 2020. – № 2. – С. 25-31.

Особистий внесок здобувача: визначено основні проблеми процесу цифровізації в Україні.

11. Котух Є.В. Реалізація національних стратегій кібербезпеки: силовий аспект // Наукові перспективи. – 2021. – № 2(8). – С. 125-136.

12. Котух Є. В. Основні підходи до забезпечення кібербезпеки: досвід країн вишеградської четвірки // Інвестиції: практика та досвід. – 2021. – № 3. – С. 68-74.

13. Котух Є.В. Проблема кібершахрайства та фактори стримування її вирішення органами публічного управління / Є.В. Котух. // Вісник НУЦЗ України. Серія: Державне управління. – 2021. – Випуск 1 (14). – С. 185-191.

14. Котух Є.В. Національні стратегії кібербезпеки: порівняльний аналіз / Є.В. Котух // Актуальні проблеми державного управління. – 2021. – № 1. – С. 48-57.

15. Котух Є.В. Оцінка рівня захисту кіберпростору в публічному управлінні: національний та організаційний виміри / Є.В. Котух // Теорія та практика державного управління. – 2021. – № 1. – С. 31-39.

16. Котух Є.В. Реалізація стратегій кібербезпеки: економіко-політичний аспект / Є.В. Котух // Теорія та практика державного управління. – 2021. – № 2. – С. 171-175.

17. Котух Є.В. та ін. Аудит інформаційної безпеки як необхідна складова управління в державних установах / Є.В. Котух, О.М. Кучма, Д.М. Нехороших, Г.В. Пліс, Г.З. Халімов // Державне будівництво. – 2021. – № 1. – Режим доступу: https://db.kh.ua/index.php/db/article/view/117/110.

Особистий внесок здобувача: визначення особливнстей аудиту інформаційної безпеки.

18. Котух Є.В. Типи владних відносин у стратегії кібербезпеки / Є.В. Котух // Інвестиції: практика та досвід. – 2021. – № 11. – С. 98-102.

19. Котух Є.В. Теоретико-методологічна модель розробки національної стратегії кібербезпеки / Є.В. Котух // Наукові перспективи. – 2021. – № 6 (12). – С. 39-52.

20. Котух Є.В. Розвиток публічно-приватного партнерства у сфері кібербезпеки // Інвестиції: практика та досвід. – 2021. – № 13. – С. 76-84.

21. Kotukh Ye.V. Public value management and new public governance as modern approaches to the development of public administration / Oleksandr O. Bryhinets, Ivo Svoboda, Oksana R. Shevchuk, Yevgen V. Kotukh, Valentyna Yu. Radich // Revista San Gregorio (Web of Science Core Collection). – Núm. 42 (2020). Pp. 205-213. http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1568/20-OLAKSANDR

Особистий внесок здобувача: визначення особливостей концепції «Public value», що має значення для розвитку концепції електронного врядування.

22. Kotukh Ye.V. Spread of virtual communities as a potential threat to state security and sustainable well-being / Viacheslav B. Dziundziuk, Oleksandr A. Kotukov, Dmytro V. Hryn, Eugene V. Kotukh // Rivista Di Studi Sulla Sostenibilita (Scopus). – 2020. – Issue 2. – Pp. 7-18.

Особистий внесок здобувача: визначено основні напрями негативного впливу розвитку віртуальних співтовариств як акторів кіберпростору на національну безпеку.

23. Kotukh Y.V. State Information Security Policy (Comparative Legal Aspect) / Y. V. Kotukh, V. B. Dziundziuk, O. M. Krutii, V. P. Solovykh, O. A. Kotukov // Cuestiones Políticas. – 2021. – 39(71). – Pp. 166-186.

Особистий внесок здобувача: визначено принципи, на яких має грунтуватись державна політика кібербезпеки.

які засвідчують апробацію матеріалів дисертації:

24. Котух Є.В. Ризики зростання відкритості публічного сектору та засоби боротьби з ними / Котух Є.В. // Збірник тез XX Міжнародного наукового конгресу «Публічне управління XXI століття: портал можливостей» (м. Харків, 23 квітня 2020 року). – Х. : Вид-во ХарРІ НАДУ «Магістр», 2020. – С. 103-106.

25. Котух Є.В. Кіберзагрози у сучасному світі / В.Б. Дзюндзюк, Є.В. Котух // International Scientific Integration ‘2020 (Seattle, Washington, USA, November 10, 2020). – Pp. 103-106.

26. Котух Є.В. Проблеми урядування у сфері кібербезпеки / В.Б. Дзюндзюк, Є.В. Котух // Abstracts of scientific papers of IV International Scientific Conference «Science and Global Studies» (Prague, November 30, 2020). – Pp. 25-28.

27. Kotukh Ye. Encryption scheme based on the automorphism group of the Ree function field / Gennady Khalimov, Yevgeniy Kotukh, Svitlana Khalimova // 7th International Conference on Internet of Things: Systems, Management and Security (Paris, France. December 14-16, 2020). – Pp. 1-8.

28. Котух Є.В. Щодо питання реалізації національних стратегій кібербезпеки / Котух Є.В. // Збірник тез XXI Міжнародного наукового конгресу «Публічне управління XXI століття: погляд у майбутнє» (м. Харків, 21 квітня 2021 року). – Х. : Вид-во ХарРІ НАДУ «Магістр», 2021. – С. 161–165.

29. Котух Є.В. Національні стратегії кібербезпеки: економіко-політичний аспект / Є.В. Котух // Multidisziplinare Forschung: Perspektiven, Probleme und Muster (Wien, 09.04.2021). – Pp. 49-50.

30. Котух Є. Боротьба з кіберзлочинністю в країнах ЄС / Є. Котух // Матеріали 18-ї регіональної науково-практичної конференції «Актуальні проблеми європейської та євроатлантичної інтеграції України» (м. Дніпро, 13 травня 2021 р.). – Дніпро : ДРІДУ НАДУ. – С. 114-117.

АНОТАЦІЯ

Котух Є.В. «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі». – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.02 – механізми державного управління. Національний університет цивільного захисту України. Харків, 2022.

Обґрунтовано, що кібербезпеку слід розглядати як суспільне благо, оскільки кібербезпека забезпечує задоволення публічних інтересів інформаційного суспільства щодо можливості належного функціонування критично важливих національних інфраструктур, і дозволяє громадянам здійснювати свою рутинну діяльність, спираючись на безпечні технології. Визначено основні виклики для публічного сектора у контексті забезпечення кібербезпеки в сучасних умовах.

Розглянуто та проаналізовано національні стратегії кібербезпеки, визначаються основні підходи до забезпечення кібербезпеки у публічному секторі. Наголошується на тому, що сфера кібербезпеки вже включена до порядку денного з питань безпеки всіх досліджених держав, але дана сфера у різних державах відрізняється за тим, як держави, по-перше, визначають

референтний об’єкт, по-друге, сприймають основні загрози та ризики та, по-третє, визначають джерела загроз та ризики.

Визначено практичні аспекти забезпечення кібербезпеки у публічному секторі, обґрунтовується необхідність формування глобального підходу до забезпечення кібербезпеки. Ключовою ідеєю при цьому виступає забезпечення кібербезпеки у середовищі Gov 2.0.

Доводено, що головними кіберзагрозами для сучасної України є крадіжка інформації, фінансове шахрайство і хакерські атаки. При цьому держава в цілому і органи публічного управління, зокрема, не є готовими сьогодні до адекватного реагування на ці загрози.

Розроблено модель інституційної кібербезпеки, відповідно до якої інституційна кібербезпека повинна мати такі основні компоненти: політика, стратегія та стандарти з кібербезпеки; управління кіберризиками; управління вразливістю та загрозами; централізоване управління інцидентами; поінформованість про кібербезпеку та освіта; управління логами та кореляція; безпечна архітектура; правові норми; технічні інструменти; безперервність діяльності; постійний аудит та моніторинг; співпраця; кіберстійкість. Обґрунтовано теоретико-методологічну модель розробки національної стратегії кібербезпеки. Визначено основні принципи публічно-приватного партнерства у сфері забезпечення кібербезпеки, до яких віднесено: перехід від «класичного» партнерства до взаємовигідної співпраці; визначення ролей членів партнерства за допомогою підходів управління ризиками; запровадження спільної відповідальності членів партнерства щодо загроз і вразливостей; впровадження системи оцінювання партнерства.

Ключові слова: публічний сектор, публічне управління, кібербезпека, кіберзагрози, формування та реалізація державної політики, органи публічної влади, електронне врядування, владні відносини, публічно-приватне партнерство у сфері забезпечення кібербезпеки.

ANNOTATION

Kotuch Ye.V. «Theoretical and methodological principles of ensuring cybersecurity in the public sector». – Qualifying scientific paper as the manuscript.

Dissertation for obtaining the scientific degree of doctor of sciences of public administration specialty 25.00.02 – Mechanisms of Public Administration. – National University of Civil Defence of Ukraine, Kharkiv, 2022.

It has been determined that ensuring cyber security is currently an important issue at all levels of public administration: from local authorities dealing with online transactions to central authorities dealing with national security issues. Cybersecurity is a dynamic goal that changes at such a rate that it is very difficult to get a completely up-to-date view of it. New cyber threats or variations of old ones emerge almost daily, as do strategies to protect against them. However, there are also some general approaches to ensuring cybersecurity, which should be defined and adapted

to the specifics of specific states and specific public authorities.

It has been proven that public sector organizations can build stronger cyber defenses by building closer relationships and collaborating with others to share experiences, mistakes, lessons learned and other information and research. The willingness to collect, analyze and share information, including about cyber incidents, is critical to improving the overall level of cybersecurity. And this requires establishing cooperation with domestic and international actors from all three sectors: public, private, non-governmental, which, in particular, will increase public awareness of cyberthreats, their dangers and methods of prevention.

The content and features of e-governance as a paradigm of public management are revealed, the concept and essence of cybersecurity in the public sector is determined, the features of the implementation of cybersecurity systems in public authorities are considered. It is justified that cybersecurity should be considered as a public good, since cybersecurity, having three main components (information and communication systems that are reliable and can withstand attacks; methods and systems for detecting threats and anomalies to ensure the stability of information and communication systems; ensuring system reactivity on cyberattacks), ensures the satisfaction of the public interests of the information society regarding the possibility of proper functioning of critical national infrastructures, and allows citizens to carry out their routine activities, relying on safe technologies. The main challenges for the public sector in the context of ensuring cybersecurity in modern conditions are identified.

An analysis of modern trends and approaches to ensuring cybersecurity in the public sector through the prism of foreign experience was carried out. National cybersecurity strategies are considered and analyzed in detail, the main approaches to ensuring cybersecurity in the public sector are determined.

It was determined that the sphere of cybersecurity is already included in the security agenda of all the studied states, but this field differs in different states according to how states, firstly, define the reference object (what needs to be protected), secondly, perceive the main threats and risks and, thirdly, determine the sources of threats and risks; according to these differences, states can be divided into two categories: states that militarize cybersecurity issues and states that criminalize cybersecurity issues.

The practical aspects of ensuring cybersecurity in the public sector are considered, the necessity of forming a global approach to ensuring cybersecurity is substantiated. The key idea here is to ensure cybersecurity in the Gov 2.0 environment. It was determined that it should be based on the implementation of the following measures: moderation of the content of public accounts; prevention of unauthorized use and transfer of confidential information; using browsers with limited privileges; implementation of intrusion detection / prevention systems; use of Web-reputation services; Universal Resource Locator (URL) and Internet Protocol (IP) filtering; filtering of malicious programs along the network perimeter; using URL shortening preview tools.

The current state and problems of preventing and countering cyberthreats in the public sector of Ukraine are analyzed. It has been proven that the main cyberthreats

for modern Ukraine are information theft, financial fraud and hacker attacks. At the same time, the state as a whole and public administration bodies, in particular, are not ready today to respond adequately to these threats. The level of cyber protection in the public sector is significantly inferior to the private sector, the public sector in general turned out to be the most unprotected from the point of view of countering cyberattacks and data leakage in Ukraine. This is due to the insufficient security of information networks, the imperfection of existing equipment and software, and the lack of qualified specialists in the field of cyber protection. Based on this, the state does not act as an entity that citizens trust in matters of cyber-protection, in particular, in relation to the protection of personal information.

It is proposed to improve the ensuring of cybersecurity in the public sector. A model of institutional cybersecurity has been developed, according to which institutional cybersecurity should have the following main components: cybersecurity policy, strategy and standards; cyber-risk management; vulnerability and threat management; centralized management of incidents; cybersecurity awareness and education; log management and correlation; secure architecture; legal norms; technical tools; business continuity; permanent audit and monitoring; cooperation; cyber resilience. The theoretical and methodological model of the development of the national cybersecurity strategy, which uses the approaches of neorealism, social constructivism, intersectionality, and cyber-Westphalia, is substantiated. The main principles of public-private partnership in the field of cybersecurity are defined, which include: transition from "classic" partnership to mutually beneficial cooperation; defining the roles of partnership members using risk management approaches; introduction of joint responsibility of partnership members regarding threats and vulnerabilities; implementation of the partnership evaluation system.

Keywords: public sector, public administration, cybersecurity, cyberthreats, formation and implementation of public policy, public authorities, e-governance, authorities’ relations, public-private partnership in the field of cybersecurity.

Відповідальний за випуск *Дзюндзюк Вячеслав Борисович*

Підписано до друку 18.08. 2022 р.
Формат 60х84/16. Обл.-вид. арк. 1,95.
Гарнітура Таймс. Наклад 100 прим. Замовлення № 79.

Надруковано в друкарні «БУКЛАЙН»
61000, м. Харків, вул. Катерининська, 46.
тел. (099) 604-49-45.
www.bookline.online