Міністерство освіти і науки України
Сумський державний університет

КАФЕДРА ЕКОНОМІКИ, ПІДПРИЄМНИЦТВА
ТА БІЗНЕС-АДМІНІСТРУВАННЯ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

Тема «Вплив кібербезпеки на розвиток інформаційної економіки»

Спеціальність 051 «Економіка»
Освітня програма 6.051.00.06 «Економіка і бізнес»

Завідувач кафедри: _____*/О.І. Карінцева/*

Керівник роботи: _____ _*/П.В. Гриценко/*

Виконавець: _____*/М.А.Чупаков /*

Група: *Едн.-81О*

Суми 2022

Анотація

Кваліфікаційна робота бакалавра містить 31 сторінку тексту; 3 розділи; 3 таблиці; список використаної літератури з 44 джерел.

Мета роботи – розкриття впливу кібербезпеки на розвиток інформаційної політики.

Відповідно до поставленої мети були вирішені такі задачі:

- проведено аналіз теоретичних засад кібербезпеки;
- проведено огляд та обґрунтування основних методів дослідження кібербезпекової політики;;
- проаналізовано основну роль кібербезпеки в розрізі цифрової економіки України.

Об’єктом дослідження є економічні категорії та поняття.

В першому розділі ми провели аналіз теоретичних засад поняття кібербезпеки, визначили основні критерії даного поняття, проаналізували основні тенденції його розвитку, а також різні підхід до його визначення.

В другому розділі нами були розглянуті основні методи дослідження кібербезпекової політики, описані їх основні складові, визначені переваги і недоліки різних методів оцінки.

В третьому розділ нами було проаналізовано і дано практичну оцінку проблематики кібербезпеки в Україні. Проведений аналіз показав, що високий рівень тісноти зв’язку (за шкалою Чеддока) між такими вище зазначеними показниками із значенням множинного коефіцієнта кореляції.

В роботі використані такі методи дослідження, як: кібернетичний, систематичний та матричний методи.

Ключові слова: кібербезпека, цифрова економіка, кібернетика, стратегія, індекс, класифікація, систематизація.

ЗМІСТ

ВСТУП

Сучасне супільство рухається в напряму формування економічно та екологічно безпечного розвитку[19, 20, 22, 24, 25, 26, 29, 30, 31, 33, 35, 38, 39, 41, 42, 43, 44]. В наш час актуальним стає питання кібербезпеки, особливо дивлячись на той буремний шлях по якому рухається зараз Україна. Глобальна кіберсфера все частіше розглядається як один із найважливіших пріоритетів безпеки України, адже його функціонування стає дедалі вагомішим фактором у розрізі військового, економічного, соціального розвитку[18, 21, 23, 27, 28, 32, 34, 36, 37, 40]. Стає все очевиднішим той факт, що мілітаризація кіберпростору неминуча, а зусилля світових держав-лідерів у бажанні попередити цей процес, залишаються малоефективними.

В Україні ці механізми поки ще залишаються на первинних етапах розвитку та становлення. Більшість з них потребують вдосконалення, проте для розробки більшості елементів та їх окремих складових бракує концептуального та практичного обґрунтування. Крім того, в нашій державі ще досі відсутні критично, життєво необхідні елементі національної стратегії кібербезпеки.

Актуальність даної тематики обумовлена необхідністю подолати суперечки між явними станом зростання проблем кібербезпеки, а також неготовності України в повній мірі адекватно відповідати новим викликам кібербезпеки.

Концептуально дана проблема, стосовно розбудови та створення ефективних засобів кібербезпеки України походить, перш за все, від відсутності законодавчо визнаних та визначених термінів, що мають чітко описати дану сферу. Не в останню чергу саме ця проблема є одним із наслідків недосконалого чинного законодавства, а також в певній мірі – своєрідною стрaдицією штучного збільшення та розширення предмету інформаційної безпеки на максимально можливу кількість сфер.

Своєрідним наслідком, що говорить про відсутність цілісності в обговоренні кібербезпекових питань у широкому колі – є проблема відсутності системної нормативно-правової бази, нормативних документів, які в повній мірі описували б загрози саме в кіберпросторі.

РОЗДІЛ 1 КІБЕРБЕЗПЕКА УКРАЇНИ: АНАЛІЗ СУЧАСНОГО СТАНУ

1.1 Стратегічна політика кібербезпеки.

Останнім часом наше суспільство все частіше та серйозніше наштовхується на різного роду кібератаки: збої та проблеми при наданні різних електронних послуг, а також блокування роботи державних органів різного рівня, сюди також можна віднести фішингові атаки електронною поштою, інші кіберзлочини та порушення цілісності, а також під загрозою опиняється конфіденційність даних, можливий інформаційно-психологічний тиск на різні рівні населення, може також бути кібертероризм та кібершпигунство, відбувається інформаційна експансія та проникнення у внутрішній національний інформаційний простір данної країни, що веде за собой блокування роботи та (або) руйнування стратегічно цінних та важливих, перш за все, для економіки а також для безпеки держави та підприємств, їх систем життєзабезпечення та функціонування й об’єктів надзвичайно підвищеної небезпеки .

Можна сказати, що критичним елементом саме соціально-економічної безпеки будь-якої, без виключення, країни є її Національна стратегія кібербезпеки (National Cybersecurity Strategy, NCS). Якщо говорити про Стратегію кібербезпеки України, то її було введено в дію саме 27.01.2016 р. Виходячи з неї можна стверджувати, що кібербезпека та інформаційна безпека мають бути визнані як найголовніші пріоритети у протидії різного роду загрозам національної безпеки. Стосовно деталізації щодо реалізації Стратегії кібербезпеки, то її відобразили у щорічних планах уряду, поглиблюючись в них, можемо помітити, що з боку органів місцевої влади передбачаються різні заходи стосовно запобігання, а також підготовки та реагування щодо можливих кіберінцидентів у рамках, що створюють ефективну національну систему підтримки кібербезпеки.

Для того, щоб координувати і контролювати діяльність різного роду суб'єктів у розрізі системи кібербезпеки має організовуватися робота відповідних державних служб, що матимуть на меті конкретні та чітко виражені зобов'язання щодо дотримання та виконання усіх вимог кібербезпеки, а саме:

– запровадили певний механізм керівництва, контролю та організації роботи Національного координаційного центру підтримки кібербезпеки, що функціонує при Раді національної безпеки та оборони України, та має на меті координацію міжвідомчої взаємодії суб'єктів національної безпеки і оборони України саме на час можливих кібератак, а також кіберінцидентів в різних інформаційно-телекомунікаційних системах та об'єктів критичної інфраструктури для того, щоб покращити ефективність системи державного управління щодо формування, а також має реалізуватися державна політика у сфері кібербезпеки на час, коли буде реалізавано Стратегію кібербезпеки України;

– є також функції державного контролю саме у сфері боротьби як безпосередньо з кіберзлочинністю, так і у розрізі кіберзахисту об'єктів важливої та критичної інформаційної інфраструктури, стосується і питань формування та реалізації також державної політики стосовно захисту у сфері кіберпростору та задіяних в ньому державних інформаційних ресурсів, а також інформація, що пзнаходиться в Державній службі спеціального зв'язку, а також питань щодо захисту інформації в Україні (ДССЗЗІ). Безпосередньо цей орган займається координацією діяльності інших суб'єктів та об'єктів, що забезпечують належний рівень кібербезпеки та в цілому кіберзахисту, а також здійснюють організаційно-технічні заходи та міри, що запобігають, виявляють та реагують на кіберінциденти та кібератаки, а також усувають наслідки. ДССЗЗІ має на меті забезпечення функціонування, так званої урядової Команди реагування на різні комп'ютерні надзвичайні події в Україні (CERT-UA) та Державний центр кіберзахисту, що безпосередньо має на меті здійснювати та впроваджувати

організаційно-технічну модель кіберзахисту та розглядає її як складову національної системи кібербезпеки в цілому по Україні. Слід зазначити, що ядром цієї моделі є не що інше, як Центр реагування на кіберзагрози (Cyber Threat Response Centre, CRC), що був створений 02.02.2018 р. і розглядається як центральний, вагомий компонент національної системи, що покликана забезпечити кіберзахист України. CRC було побудовано на основі найновітніших досягнень та здобутків у розрізі кібербезпеки вітчизняних, а також провідних ІТ-компаній світу. Створені та розроблені на рівні кращих світових аналогів такі поняття, як сучасна технологічна, а також аналітична системи CRC мають на меті закономірно претендувати на звання найпотужнішого представника в європейському співтоваристві, в цілому. Іншою важливою функцією ДССЗЗІ, що пов’язана безпосередньо з контролем та базуються на дотриманні різного роду вимог законодавства у сферах електронних та електронних довірчих послуг, займаються також наглядом за кваліфікованими постачальниками інших електронних довірчих послуг, так і у галузі криптографічного захисту важливої інформації. Бо переважно гарантувати конфіденційність та цілісність інформації, захищати інформацію від несанкціонованого доступу мають основну вимогу - успішну реалізацію електронного документообігу насамперед між державними установами, а також громадянами та різними суб’єктами приватного сектора економіки;

– якщо говорити про сьогоднішній день, то питання захисту персональних даних громадян потребує вирішення, як і питання конфіденційності даних компаній, тому в Україні було створено відповідно такий незалежний державний орган, що являється наглядовим, у відповідності до вимог Конвенції Ради Європи щодо захисту осіб у зв’язку з автоматизацією обробки персональних даних. Контролем за дотриманням законодавства стосовно підтримки захисту персональних даних покликаний займатися Уповноважений Верховної Ради України з прав людини;

– організація роботи Департаменту кіберполіції Національної поліції України, що займається спеціалізацією попередження, виявлення, припинення, а також розкриття різного роду кримінальних правопорушень, а також розглядає механізми підготовки, щодо вчинення та приховування яких може передбачати використання комп'ютерної техніки та систем телекомунікацій, а також комп'ютерних мереж ;

– створення компетентного органу у сфері інформаційної та кібербезпеки;

Державним агентством з електронного врядування України проводиться контроль вимог до кібербезпеки операторів. Постачальниками цифрових послуг та операторами основних служб у відповідності до ст. 5 Закону України про кібербезпеку здійснюється управління кіберризиками та реалізовуються конкретні заходи щодо забезпечення кібербезпеки і повідомляються про різні випадки кіберінцидентів відповідні державні органи.

1.2 Цілі та пріоритети кібербезпеки України.

Президентом України Володимиром Зеленським, а саме Указом № 447/2021 від 26 серпня 2021 року затверджено рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України».

Стратегією кібербезпеки України визначається пріоритетність у питаннях національних інтересів у розрізі кібербезпеки, стосовно наявних та потенційно можливих кіберзагроз, цілей та завдань забезпечення кібербезпеки України, щоб мати на меті створення сприятливих умов для максимально безпечного функціонування кіберпростору в цілому, а також його використання продиктованими інтересам осоіб, суспільства і держави в цілому.

У цій Стратегії чітко визначається той факт, що «забезпеченням

кібербезпеки має визначатися як один з найбільш пріоритетних у системі національної безпеки нашої держави. Реалізацію зазначеного пріоритету повинно здійснювати безпосередньо посиленням можливостями національної системи кібербезпеки протидіяти кіберзагрозам у сфері сучасного безпекового середовища».

Наголошуємо, що «Кіберпростір, разом з іншими фізичними просторами, розглядається як одна з можливих сфер військових дій. Посилюється тенденція до створення кіберармії, до завдань якої входить не тільки захист критично важливих інформаційних інфраструктур від кібератак, а й проведення профілактики у кіберпросторі».

Оцінку дій держави-агресора надано тому, що «Російська Федерація залишається у позиції одного із основних джерел загрози національній та міжнародній кібербезпеки, активно реалізуючи концепцію інформаційної війни на основі поєднання кіберпростору та інформаційно-психологічних диверсій, механізми якого активно використовувалися у гібридній війні проти нашої держави».

Очікується зростання інтенсивності міждержавного протистояння та розвідувально-підривної діяльності Росії в кіберпросторі України. Розширення кола держав, що мають на меті формування власної кіберрозвідки, опанувати сучасні методи розвідки та підривної діяльності в кіберпросторі, посилити державний контроль над державною частиною Інтернету. Водночас поширюється інструментарій, що посилюється тенденція розвідувально-підривної діяльності в кіберпросторі через здійснення кібервпливу спецслужбами та міжнародними хакерськими угрупованнями за участю окремих країн (переважно Російської Федерації). Стратегія також підкреслює, що використання кіберпростору терористичними групами стає глобалізованим.

Стратегія визначає основні виклики та загрози, з якими стикається Україна у сфері кібербезпеки.

Основними викликами для України у сфері кібербезпеки є:

– активним є використанням кіберзасобів у міжнародній конкуренції;
– змагальним характером для розвитку засобів кібербезпеки в нинішніх умовах швидких та прогресуючих змін в сфері інформаційно-комунікаційних технологій, а також хмарних обчислень, 5G-мереж, великих пластів даних, також штучного інтелекту та ін.;
– важливим аспектом є мілітаризація кіберпростору України та проведення розвитку кіберзброї, що дасть нам можливість приховати проводення кібератак для підтримки активних бойових дій і проводити розвідувально-підривну діяльність у кіберпросторі ворога;
– мінімізація впливу пандемії COVID-19 безпосередньо на економічну діяльність, а також соціальну поведінку, спричинену стрімкою трансформацією та організацією великого об'єму пласту суспільного рівня відносин у розрізі дистанційного режиму з використанням широкого асортименту електронних сервісів, а також інформаційно-комунікаційних систем України;
– процес впровадження в роботу нових технологій, а також цифрових послуг, конкретних механізмів можливостей електронної взаємодії між громадянами та громадян з державою здійснюватимуться безсистемно безпосередньо в частині заходів, що стосуються питань кібербезпеки та відсутні належні оцінки ризиків кібербезпеки.

Саме цим документом стратегічного характеру передбачається формування основних засад, що важливі при розбудові національної системи кібербезпеки України. Розшифруємо, основними суб'єктами національної системи кібербезпеки України є залучення до широкого колоа учасників до розв'язання проблем кібербезпеки, враховуючи суб'єкти господарювання, а також громадські спілки та об'єднання, включаючи окремих громадян нащої держави. Ключовим моментом, що об'єднає та скоординує цей процес будує Національний координаційний центр кібербезпеки України.

Визначимо пріоритети, завдяки чому досягнеться забезпечення кібербезпеки України:

- убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;
- захист прав, свобод і законних інтересів громадян України у кіберпросторі;
- європейська і євроатлантична інтеграція у сфері кібербезпеки.

Питанням формування принципово нової якості в розрізі національної системи кібербезпеки вимагає принципово чіткого, конкретного та зрозумілого визначення саме стратегічних цілей, які будуть досягатися в період реалізації саме цієї Стратегії.

Для того, щоб сформувати потенціал для стримування (С) необхідно досягти таких стратегічних цілей:

ціль С.1. Досить дієва кібероборона;

ціль С.2. Необхідна ефективна протидія щодо розвідувально-підривної діяльності;

ціль С.3. Продуктивна протидія кіберзлочинності;

ціль С.4. Планування та розвиток асиметрично визначеній інструментів стримування кіберзлочинності.

Для того, щоб досягти високого рівня кіберстійкост (К) необхідно є досягти таких стратегічних цілей та задач:

ціль К.1. Побудова національної кіберготовності та вистроїти надійний кіберзахист;

ціль К.2. Професійно вдосконалити кіберобізнане суспільство;

ціль К.3. Налаштувати безпечні цифрові послуги.

Для того, щоб вдосконалити взаємодію (В) необхідно досягти таких стратегічних цілей та задач:

ціль В.1. Зміцнити систему координації;

ціль В.2. Сформувати нову модель відносин у розрізі кібербезпеки;

ціль В.3. Ефективне прагматичне міжнародне співробітництво в сфері кібербезпеки.

Стратегія визначає напрями розвитку в зовнішньополітичній діяльності України у сфері встановлення кібербезпеки. «Україна у розрізі кібербезпеки забезпечує поглиблену євроінтеграцію в процесі уніфікації підходу, методу і засобу, щоб забезпечити кібербезпеку в альянсі з ЄС і НАТО, встановлення та узгодження заходів разом з ключовими іноземними партнерами, що допоможуть спрямувати та посилити кіберстійкість України, спровокувати розвиток спроможностей заради налагодження національної системи кібербезпеки та захистити національні інтереси у кіберпросторі Україні», — говориться в документі.

Координувати реалізацію Стратегії буде робочий орган Ради національної безпеки і оборони України — Національний координаційний центр кібербезпеки.

Реалізацією Стратегії буде займатися основним суб'єктом національної системи кібербезпеки, Міністерство закордонних справ України, а також Міністерство цифрової трансформації України, Міністерство освіти і науки України, окрім цього інші суб'єкти забезпечать кібербезпеку в межах їхньої прямої компетенції.

Фінансуванням заходів щодо реалізації Стратегії здійснюватиме в межах видатків.

Стратегія буде ґрунтуватися безпосередньо на положеннях Конституції України, законами України «Про національну безпеку України» та «Про основні засади забезпечення кібербезпеки України», Конвенціями про захист прав людини і основоположних свобод.

РОЗДІЛ 2 МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ

2.1 Аналіз методології.

Актуальністю теми обумовлена необхідність побудувати валідну наукову модель щодо дослідження кібербезпеки. Говорячи про практичне русло, можна зазначити, що це допоможе грамотно зрозуміти безпосередньо природу даного процесу, а також дає можливість сформувати ефективні прогнозні моделі для того, щоб побудувати організаційно-функціональну структуру для розвитку національної системи кібербезпеки. Давайте розглянемо саме евристичні можливості стосовно кібернетичного, а також системного та матричного підходів, як інструментів метродологічного дослідження самого процесу кібербезпекової політики. Дамо визначення, кібернетика (від грецьк. мистецтво управління) – це наука, що говорить про загальні закони отримання, а також збереження та передання і що немало важливо розповсюдження конкретної інформації в складних для управління системах.

Також слід розуміти, що під управляючими системами можуть розумітися не тільки технічні, але будь-які як біологічні, так і соціальні системи. Приклади складних управляючих систем виступатимуть у вигляді нервових систем живих організмів, перш за все людини, а також апарат в управлінні суспільством. Людським суспільством використали як прикладом в цьому визначенні. Приймаючи до уваги цей недолік, Н.Вінер в свій час опублікував у 1954 році свою нову книгу «Кібернетика і суспільство». Для написання цих книжок Вінер використав характерний оповідний підхід, описуючи власні думки і враження стосовно деяких досліджень, що він виконував разом зколегами в галузі теорії випадкових процесів, а також фізіології нервової системи. Без перебільшення вона не містила послідовного та конкретного викладу методів нової науки, а також її результати.

Англійський вчений У.-Р.Ешбі більш конкретно та систематично виклав суть кібернетики у 1956 році. В цілому, розвиток кібернетики у США та Західної Європи, був характерним захопленням її саме філософськими аспектами.

Проте водночас розгортанням та використанням цифровими обчислювальними машинами у 50-х рр. XX століття вимагало створення наукових основ для безпосередньо проектуваннями такими машинами і системами.

2.2 Кібернетичний, системний та матричний підходи.

Кібернетичними підходом, розглянутим окремими дослідниками, виступав частково визнаним науковим методом його дослідження. Проте якщо все ж придивитись на період такого зіставлення та поєднати його з періодизаціями у розвитку кібернетики, прослідковується той факт, що ця тенденція найбільш яскраво припадала на другий з періодів в розвитку кібернетики, а саме на 60-ті роки XX століття, в час коли наука все ще перебувала в тій стадії, коли тільки стверджувалась та розповсюджувалась, тоді ще точилися дуже жваві дискусії стосовно потреби в її існуванні. Бо з початку 70-х років, саме коли кібернетика вже все-таки остаточно закріпилась і виокремилась як окрема наука, цей підхід не був таким беззаперечним. А в кінці1990-х років остаточно сформувалась позиція, виходячи з якої кібернетика вже повністю охопила не тільки лише теорію цифрових та обчислювальних машин, але й чисельно застосовувалась в різних областях та сферах, з початку автоматизації в обробці наукових даних, закінчуючи управлінням великими економічними та соціальними-економічними системами. Виходячи з цього, можна сміливо виділяти три таких компоненти кібернетики: теоретична кібернетика, що має на меті досліджувати філософські й математичні проблеми кібернетики; технічна кібернетика, що досліджувала принципи та розробку технічні системи, що

фактично були побудовані в кіберпросторі; прикладна кібернетика, що досліджувала можливість використати ідеї та методи, а також технічні засоби кібернетики для того, щоб вирішити практичні завдання у різних сферах та зонах життєдіяльності людини. Фактичним показником елементарної схеми управління слугувала самоорганізація штучного інтелекту: вся інформація передавалась від суб'єкта управління до безпосередньо об'єкта за допомгою каналів прямого зв'язку; канали зворотного зв'язку отримували інформацію саме від об'єкта управління до суб'єкта; виходячи з цього на підставі отримання інформації відбувалось корегування і корекція конкретного алгоритму управління системою. Можливістю накопичувати інформацію в управляючі системи, а також здійснити складні її перетворення, реалізувалось за допомогою створення ЦОМ, та була зумовлена можливістю сформувати і втілити в життя вирішення завдань не лише тільки фізичної, але й розумова діяльність людини. Теоретичною базою кібернетики має збагачувати примноження дискретних форм уявлення конкретної інформації. Також завданням теоретичної кібернетики є створення принципово нового наукового апарату і методів дослідження, що мають бути придатними для того, щоб вивчити широкі класи та шари системи управління в незалежності від їх природи буття. Виходячи з цього, теорією інформації, що має вивчати кількісну міру інформації, являється однією із наукових напрямків та шляхів,для того щоб брати основу теоретична кібернетика.

Одночасно з цим теорією кодування і теорією створення алгоритмів, що мають вивчати та подавати дискретну інформацію у формі послідовності та перетворювати такі послідовност. Безпосередньо в рамках кібернетики були вперше проведені дослідження гібридних систем та на основі поняття кібернетика був розроблений чіткий алгоритм щодо ведення гібридної війни, методами виступали: теорія випадкових процесів; також теорія ігор; не забуваємо про теорію статистичних рішень; поширеними були методи вирішення складних екстремальних завдань (стохастичне, лінійне, а також

динамічне програмування); теорія графів. За безпосередньою допомогою цих теорій стало можливим впритул приблизитись до розкриття системи закономірності накопичення, а також перетворити інформацію в мозку у людини. Дуже важливим, на наш погляд, є методологічні інструменти за допомогою яких проводиться експеримент і комп'ютерне моделювання.

Виходячи з вище сказаного, можемо сказати, що специфічним предметом дослідження формувалися особливі для нас нові методи дослідження, що знайшли свої застосування також в багатьох інших науках, що не залежить також від специфічності об'єктів, що нами вивчаються. Ще на початку легалізація кібернетики дослідниками були зроблені кроки для знаходження відповідей в процесі пошуку шляхів в розвитку штучного інтелекту.

Такими межами неможливо орієнтуватися.

Дуже складними завданнями для штучного інтелекту буде така здатність:

– самостійно намагатися задавати собі завдання, а також робити таймінг для їх реалізації, здійснення пошуку пріоритетності завдань для того, щоб досягти загальних цілей функціонування системи;

– встановити загальні цілі та задачі в розвитку всього виду кіборгів;

– оцінити та отримати результати стосовно вирішення питання вдосконалення системи управління в цілому.

Важливим значенням буде застосування саме системного підходу, що за допоможе уможливити розгляд предметів дослідження як безпосередньо певну конкретну систему, що має складатися із певної сукупності елементів та взаємозв'язків між ними, що в свою чергу створять нову якість у своїй єдності. Застосуватися даний підхід буде у відображенні в численних та експерементальних дослідженнях. Його активно використає в свої роботах В.А. Ліпкан, саме він запропонує розглянути систематизацію інформаційного законодавства системно та складати її з таких систематино поєднаних елементів, таких як інкорпорація, консолідація, а також кодифікація, а якщо

говорити про саме інформаційну політику держави, то слід зазначити, що це є складною системою, що пов’язана між собою однорідними суспільними відносинами у сфері інформації.

Даним методом також можна знаходити своє відображення В.С. Цимбалюком безпосередньо формувати теоретично-правові засади стосовно предмета, а також метода на основі системи інформаційного права, що представляє собою основу формування теорії кодифікації законодавства.

Використовуючи методологію у вигляді системного підходу, зазначимо, що дослідження статичних, динамічних, структурних компонентів, онтогенетичних зв’язків та властивостей кібернетичних відносин, а також їхні, не тільки внутрішні, але зовнішні вияви, виявили певний високий рівень інформаційної взаємодії безпосередньо з інформаційним середовищем.

До основних методологічних положень системного підходу під час дослідження проблематики кібернетичної безпеки і відповідних відносин у рамках реалізації кібербезпекової політики належать:

– кібернетичнами відносинами та їхніми окремими компонентами розглядаються системи (підсистеми); вони мають за основу цілісний характер, що має зумовлювати їх безпосереднє виокремлення із сфери зовнішнього середовища та має об’єднювати в сталі кібернетичні зв’язки.

У відповідності до кібербезпекової політики це поняття має інтерпретуватися багатошаровою, комплексною, узгодженою за метою, а також завданням та принципом діяльності у відповідності до суб’єктів національної системи забезпечення кібербезпеки;

– елементами системи має взаємопов’язуватися кожне конкретне явище зі сталою множиною інших конкретних систем, таким чином, щоб властивості елементів (підсистем) залежали від властивостей одного цілого, частиною такого цілого вони і є, саме тому забезпечити кібернетичну безпеку та вплив має основну задачу обумовлючи ефективну реалізацію державної кібербезпекової політики, адже усвідомлення залежності від особливостей

його процесів взаємодії з іншими схожими складниками певних конкретних системних утворень поєднується з іншими видами кібернетичних відносин в системі.

– залежність своєрідності природи та системності тієї чи іншої підсистемисистеми, може завдавати як певний ракурс процесу його вивчення, так і відповідність властивостям; кожен вид суспільних відносин повинен мати певну динамічну природу, саме тому і в кібернетичних відносинах мають місце властивості таким ознакам системності, як процеси виникнення, а також становлення, окрім цього розвитку, не забуваючи про зміни та припинення існування;

– процес функціонування та розвитку кібернетичних відносин має здійснюватися у відповідності до результатів кібернетичної взаємодії напряму із зовнішнім середовищем за умови домінування внутрішніх закономірностей, в першу чергу, над зовнішніми чинниками, а також закономірностей. Це може означає тільки те, що сталістю даних елементів зсередини системи можуть бути кібернетичні відносини, стосовно рівня цих зв'язків між елементами виступають вищі за будь-який рівень зв'язку певного елемента з елементами іншої системи та ії підсистеми, наприклад, можемо привести інші суспільні відносини. Безпосередньо з цим і асоціюються формування кібермови, в особливості її конотаціями, кіберкультурою та кіберсоціумом. Зважаємо на високу складність та певну новизну кібернетичних правовідносин, не можемо залишити позаду і матричний підхід. Беручи до уваги теорію інформаційного права, а саме такий методологічний підхід, то він був запозичений із правової інформатики і мав найбільше використання в роботах такого українського вченого, як В.С. Цимбалюк.

Виходячи з робіт науковця, підкреслюємо, що застосовуючи матричний підхід моделювання саме інститутів правового регулювання, що дає можливість визначити його межі для застосуванн, стосовно структуризації загальновизнаних теоретичних та практичних окремих та конкретних

інститутів не тільки інформаційного права, але і в тому числі тих, що мали на меті знаходження відображення у певних спеціальних юридичних законах, перш за все, за загальною та особливою, а також спеціальною частинами цього права, що в перспективі мали екстраполювати свою проекцію на структуру проекту Кодексу України про інформацію та кібербезпеку .

Натомість В.С. Цимбалюк не досить чітко формулював зміст даного підходу, його алгоритм щодо наукового застосування, а також, беручи до уваги, можливості та прогнози стосовно наслідків у вигляді певних очікуваних результатів, можуть порівнювати його лише з таким методом формування таблиці, як таблиця Д.І. Менделєєва. Зазначимо, що проведені нами дослідження можуть дати змогу констатувати, що саме матричний підхід в свій час був запозичений інформатикою з такої науки, як математика і в той же час розвивався в аналітичній геометрії.

Активним використанням його були потреби у формуванні та дослідженні економічних моделей. Цей підхід знайшов адаптацію інформатикою в структуризації саме кібернетичних процесів у соціальних та економічних системах та мав на меті формалізацію з метою автоматизувати та застосувати комп'ютерниі кібернетичні технології.

У такій науці, як математика матрицею, як правило, називають прямокутні таблиці чисел, що можуть мати відповідні рядки, а також стовпчики векторів, що проходять аналіз, як по горизонталі, так і по вертикалі, а також по діагоналях тощо. Щодо нашого з Вами дослідження, то тут слід зазначити, що матричний підхід ми маємо інтерпретувати як саме стандартний спосіб для структуризації та зібрання даних, основуючись на такій моделі, як «об'єкт – ознака». Кожен об'єкт аналізу має характеризуватися, як свій ряд, а кожна ознака – свій конкретний стовпчик. У відповідності до матричного підходу встановлюються та розвиваються кібернетичні відносин для описання будь-якого соціального явища за допомогою багатокритеріальних параметрів безпеки та мають, як правило, безсумнівно позитивні, але можуть мати і певні негативні наслідки.

РОЗДІЛ 3 КІБЕРБЕЗПЕКА ТА СТАНОВЛЕННЯ ЦИФРОВОЇ ЕКОНОМІКИ: ПРОБЛЕМИ ВЗАЄМОЗВ'ЯЗКУ.

3.1 Постановка проблеми кібербезпеки в розрізі цифрової економіки

За допомогою цифрових технологій можна безумовно підвищити не тільки ефективність створення певного суспільного продукту, але і задовольнити потреби людей, збалансувати і використати виробничі, технологічні, трудові, інтелектуальні, фінансові та природних ресурси, що є предтечею для виникнення фактично та особливо нового укладу життя суспільства, так званої – «цифрової економіки». Її ключовими технологіями є: «Великі дані» («Big data»), також «Хмарні обчислення» («Cloud computing»), не забуваючи про «Інтернет речей» («Internet of Things»), все це дозволяє зібрати, зберігти, обробити і проаналізувати великі масиви цифрових даних принципово різного походження, оцінити їх повноту і характер, використовуючи їх для подальшої оптимізації більшості бізнес-процесів, швидко ухвалити оперативні та стратегічні рішення, як окремих компаній, а також цілих країн, так і гнучко і адекватно реагувати на різного роду кон'юнктурні зміни, а також на запити ринку навіть при одночасному зменшенні їх впливу на суб'єкт людського фактору в процесі управління і ухвалювати рішення в будь-якій, без виключення, сфері господарської діяльності і не тільки, а й суспільного життя. Натомість, поряд із перевагами та вигодами цифровізація може утворювати цілий ряд кіберзагроз для діяльності не тільки на рівні країн, але і на рівни компаній, а також окремих громадян. Використовувати ІК-технології для несанкціонованого та протиправного заволодіння даними як юридичних, так і фізичних осіб сторонніми об'єктами та суб'єктами можливо нанесення значної шкоди та проблем функціонування господарської діяльності – виведення з ладу великих систем управління компаній, дає можливість в позбавленні їх майна та коштів, може блокувати та паралізує виробничий процес, мінімізує

ефективність економіки в цілому. Якщо говорити про, наприклад Україну, то в даному випадку Рада національної безпеки і оборони нашої з Вами держави в свій час заявляла, що у 2020 році в країні мають бути виявлені понад один мільйон різних кіберзагроз. Як правило частіше за все, жертвами хакерів можуть ставати приватні фірми та підприємства. Кіберзлочинці мають на меті активно використовувати та спробують сканувати мережу, частішають мережеві атаки прикладного та інших рівнів, бувають спроби WEB-атак, також частим є фішинг, DDoS-атаки, поширюється шкідливе програмне забезпеченнятощо. Злочинці полюють за різного роду даними. В той же час одні хочуть вкрасти особисту закриту конфіденційну інформацію, що знаходиться в компанії; інші злочинці привласнюють її гроші. В той же час основою для кібератак часто є отримання та здобуток неправомірної фінансової вигоди або крадіжка грошей підприємства/клієнта, викрадається інформація, що становитиме загрозу у вигляді компромату на компанію, що може в свою чергу дозволити використовуючи шантаж отримати від неї певну фінансову вигоду. Подібним чином, часто загрожують тероризувати усі без виключення країни світу, не тільки Україну, а проблемою кібербезпеки є неабияка гострота і важливість постановки даної проблеми. Є певна тенденція - невпинно зростає розмір світового ринку кібербезпеки, що вже у 2020 р. оцінюється у розмірі 173 млрд дол., а до 2026 р. маємо очікування його росту більше ніж вдвічі – до 270 млрд дол. З цього можемо зробити висновок, що подальший розвиток цифрової економіки і її ефективність, а також отримання людьми всіх її переваг нерозривно пов’язується нами із одночасною розбудовою та формуванням відповідних систем кібербезпеки.

3.2 Методи та етапи вирішення проблеми взаємозв’язку

Вивченням важливості забезпечення належного рівня кібербезпеки для розвитку безпосередньо цифрової економіки займаються ряд зарубіжних

науковців та присвячено безліч наукових робіт. В часто відзначають, що необхідно заради успішного та ефективного розвитку цифрової економіки забезпечити надійний цифровий простір, досягти чого можливо тільки за рахунок вдосконалення до відповідності рівню законодавства і політики у розрізі та сфері кібербезпеки, до речі доводиться такий факт, що кіберзагрози можуть уповільнювати темпи розвитку саме цифрової економіки. Дослідженнями британської аудиторської компанії «Ernst & Young» ми побачили, що серйозними прогалинами у сфері кібербезпеки переважно на рівні компаній в цілому по всьому світу, будуть такі, що недостатньо усвідомлені керівництвом, так і в цілому у зв'язку з відсутністю досить ефективними організаційними і технічними засобами протидії кіберзагрозам в системі. Натомість їх дослідженнями здебільшого займалися у сфері правового регулювання та сформували систему інформаційної безпеки нашої держави, в той же час маловивченими залишаються питання впливу кібербезпеки в цілому на формування та розвиток цифрової економіки України.

Одним з ключових факторів та проблем пов'язаних зі становленням цифрової економіки, основою якої саме інформація стає ключовим ресурсом, має бути забезпечення кібербезпеки. В узагальненому вигляді під поняттям кібербезпека ми розуміємо сукупність таких спеціальних правових, а також організаційних, і технічних заходів, фактор реалізації яких дасть нам змогу надійно забезпечити захист інформаційних та комп'ютерних систем, а також мереж та різного роду програмних додатків, перш за все, від кібернетичних атак зловмисників. Саме такі атаки можуть завдати критичної шкоди та колосальних матеріальних збитків як підприємствам, так і в той же час через втрату коштів і активів або через розкриття важливої конфіденційної комерційної інформації та таємниці, так і в цілому державі – є вірогідність провокацій техногенних катастроф, спричинення збитків для цивільної, фінансової, а також енергетичної та військової інфраструктури (табл. 1). З поширенням цифровізації, а також і комп'ютеризації передусім у

виробництві, але часто і у побуті, масштаби кіберзагроз можуть серйозно зростати та бути пропорційно розширеними спектрами продуктів і послуг, переважно де застосовуються інформаційні технології. Вже сьогодні, за оцінками експертів, у світі налічується вже близько шести тисяч тіньових ринків, де часто можуть продавати близько 45 тис. продуктів або послуг для того, щоб здійснювати кіберзлочини, а найшвидше та найбільше зростаючим ринком у цій сфері наразі є ринок послуг зі зламу комп'ютерних програм та систем.

Таблиця 1

ТОП-10 найбільш цінних для зловмисників типів даних та найбільш актуальних для компаній кіберзагроз у світі, 2018–2019 р., відсотків у загальній кількості

	Типи даних, цінні для зловмисників	%	Кіберзагрози для компаній	%
1	Клієнтська інформація	17	Фішинг	22
2	Фінансова інформація	12	Шкідливе ПЗ	20
3	Стратегічні плани	12	Кібератаки з метою дезорганізації діяльності	13
4	Інформація про вище керівництво	11	Кібератаки з метою викрадення коштів	12
5	Паролі клієнтів	11	Шахрайство	10
6	Результати НДДКР	9	Кібератаки з метою викрадення об'єктів інтелектуальної власності	8
7	Інформація про угоди злиття та поглинання	8	Спам	6
8	Об'єкти інтелектуальної власності	6	Атаки зсередини організації	5
9	Незапатентована інтелектуальна власність	5	Стихійні лиха	2
10	Інформація про постачальників	5	Шпіонаж	2

Таблиця 1. Збитки для цивільної, фінансової, енергетичної та військової інфраструктури

З огляду на те, що гарантія кібербезпеки є актуальною задачею для держави і бізнесу, в цілому, а розробка системи адекватних заходів протидії даним викликам і загрозам можуть стати важливими напрямами науково-технічного прогресу і адекватної державної політики в сфері кібербезпеки. Для оптимального моніторингу та побудови порівняльної оцінки ступеня готовності країни саме до захисту даних в кіберпросторі використовують такі показники «Глобальний індекс кібербезпеки» (Global Cybersecurity Index, GCI) та «Національний індекс кібербезпеки» (National Cyber Security Index,

NCSI). Ці індекси мають оцінювати ризики для корпоративної, а також промислової та урядової інформаційної та економічної інфраструктури від будь-яких кіберзагроз. Для формування Індексу NCSI мають враховуватися такі ключові кіберзагрози, а саме: втручання в систему певних електронних послуг (послуги недоступні), також порушення системи цілісності даних (несанкціоноване внесення змін), виділемо також порушення конфіденційності даних (оприлюднення таємниці). Завдяки рейтингу NCSI може збудувати вимірювання саме тих аспектів кібербезпеки, що відображаються в урядових рішеннях і мають стосуватися спеціальних законодавчих, а також нормативно-правових актів, при наявності яких розвиваються спеціальні інституції, що базуються на протидії загрозам, а також організації співпраці між різного роду суб'єктами стосовно протидії загрозам, при наявності певних відповідних технологічних можливостей і програмного забезпечення та ін. Використання такого підходу дозволяє нам отримати чітку та конкретну верифіковану основу для складання індексу і є його відмінною рисою. Він вибудовується на основі відповідей експертів щодо стану безпеки кіберпростору у розрізі законодавчої, технічної та організаційної складових, а також оцінювання можливостей підвищення їх потенціалу та взаємодії (табл. 2).

Таблиця 2

Структура формування Глобального індексу кібербезпеки (GCI)

Складові	Зміст складових
Законодавство	Законодавство з кіберзлочинності; регулювання кібербезпеки; законодавче обмеження спаму
Технічне забезпечення	CERT / CIRT / CSIRT*; структура застосовуваних стандартів; органи стандартизації; технічні механізми і можливості, що застосовуються для боротьби зі спамом; використання хмари для забезпечення кібербезпеки; механізми захисту дітей від негативної інформації в Інтернеті
Організаційна складова	Національна стратегія кібербезпеки; відповідальні органи; показники кібербезпеки
Підвищення потенціалу	Кампанії з інформування громадськості; структура для сертифікації та акредитації фахівців з кібербезпеки; професійні тренувальні курси з кібербезпеки; освітні програми або академічні курси з кібербезпеки; програми наукових досліджень і розробок в галузі кібербезпеки тощо
Кооперація	Двосторонні угоди; багатосторонні угоди; участь в міжнародних асоціаціях; державно-приватне партнерство; міжвідомче /внутрішньовідомче партнерство тощо

Таблиця 2 Структура формування Глобального індексу кібербезпеки

Аналіз індексу дозволяє зробити висновок, що законодавча база є ключовою у забезпеченні кібербезпеки. Юридичний контекст оцінюється на основі кількості правових інститутів і структур, відповідальних за кібербезпеку. Забезпечення останньої неможливо здійснити без відповідних технічних навичок для виявлення кібератак і реагування на них. Для того, щоб забезпечити ефективне функціонування системи кібербезпеки важливими елементами є: наявність національної стратегії; наявність моделі управління, адекватний рівень вирішення задач; органи нагляду, що укомплектовані відповідними експертами та фахівцями. Все перераховане має становити основу для ефективної організаційної складової кібербезпеки на івні держави. Можливостями підвищення даного потенціалу, а також рівня кібербезпеки необхідно оцінювати за кількістю та якістю досліджень і розробок в даній конкретній сфері, важливою є наявність освітніх і навчальних програм, немало важливим аспектом є наявність сертифікованих фахівців та установ державного сектору. Для того, щоб забезпечити максимальний рівень ефективності в боротьбі із кіберзлочинністю важливою умовою є передусім розширення та покращення співпраці на національному та міжнародному рівнях, що має оцінюватися безпосередньо за кількістю партнерств з обміну інформацією. Рівнем цифрового розвитку (Digital Development Level – DDL) максимально коректно розраховути Індекс розвитку ІКТ (IDI) та Індекс мережевої готовності (NRI). Індекс розвитку ІКТ (IDI) можемо визначити за показниками розвиненості інфраструктури саме інформаційних технологій. Метою його призначення є моніторинг розвитку ІТ у країнах, а також їх позиціонування на світовому ринку ІТ маючи такі три субіндекси, а саме: доступ, використання, навички. Зазначимо, що індексом мережевої готовності, як правило, складає з чотири субіндекси, що можуть оцінити середовище для розвитку ІТ, розраховує готовність суспільства використовувати ІТ та їх фактичне використання на рівні держави, бізнесу, населення, а також всі наслідки, що ІТ може породжувати в економіці та суспільстві в цілому. Перші три субіндекси – це такі драйвери зростання, які

формуються на основі передумов для четвертого субіндексу, а саме – впливу ІТ на економіку. Якщо порівняємо країни за відповідними індексами цифрового розвитку рівню кібербезпеки, взаємозв'язок стає напрочуд очевидним (табл. 3)

Таблиця 3

Рейтинг країн за індексами кібербезпеки та розвитку цифрової економіки

Національний індекс кібербезпеки, 2019			Глобальний індекс кібербезпеки, 2018			Рівень цифрового розвитку (DDL)*, 2019	
Рейтинг	Країна	Оцінка	Рейтинг	Країна	Оцінка	Країна	Оцінка
1	Греція	96,10	1	Велика Британія	93,1	Швейцарія	85,13
2	Чеська Республіка	92,21	2	США	92,6	Республіка Корея	84,25
3	Естонія	90,91	3	Франція	91,8	Ісландія	84,19
4	Литва	88,31	4	Литва	90,8	Великобританія	83,96
5	Іспанія	88,31	5	Естонія	90,5	Нідерланди	83,88
6	Бельгія	85,71	6	Сінгапур	89,8	Норвегія	83,78
7	Словаччина	83,12	7	Іспанія	89,6	Данія	83,55
8	Хорватія	83,12	8	Малайзія	89,3	Швеція	83,48
9	Франція	83,12	9	Норвегія	89,2	Сінгапур	83,11
10	Фінляндія	81,82	10	Австралія	89,2	Люксембург	83,06
11	Данія	81,82	11	Люксембург	89,0	США	82,33
12	Нідерланди	81,82	12	Нідерланди	88,5	Фінляндія	82,26
13	Сінгапур	80,52	13	Саудівська Аравія	88,1	Японія	82,15
14	Німеччина	80,52	14	Японія	88,0	Німеччина	81,95
15	США	79,22	15	Республіка Корея	87,3	Нова Зеландія	80,94
…			…	…			
29	**Україна**	**63,64**	**54**	**Україна**	**66,1**	**Україна**	**58,10**

Таблиця 3 Рейтинг країн за індексами кібербезпеки

У відповідності до рейтингу NCSI-2019 Україна посідає 29 місце серед всіх країн. В списку сильних сторін можна сміливо виділити та відзначити серйозні та потужні напрацювання у сфері запровадження та втілення в життя політики кібербезпеки, що впливає на захист персональних данихА також допомагає у боротьбі з кіберзлочинністю. Натомість слабкими сторонами продовжують залишатися позиції управління над інцидентами та кіберкризами, захист електронних сервісів, аналіз, а також та інформування громадськості про можливі та існуючі кіберзагрози. Наші сусіди по карті, – а саме, деякі країни пострадянського простору, – все ж-таки мають кращі позиції у рейтингу, аніж Україна. Фактично у першу десятку лідерів входять Чеська республіка (2), Естонія (3) та Литва (4). Світовими лідерами рейтингу Глобального індексу кібербезпеки у 2018 році стали Велика Британія, друге місце опанували США, а третю – Франція. Наша держава в той же час опинилась у шостій десятці країн, але посіла 54 місце. В той же час такий

результат можна оцінити як прогрес, адже у попередні роки ми посідали мали значно нижчі позиції, щодо ж поліпшення рейтингу, то тут не обійшлося без наполегливої роботи держави над створенням чіткої системи адекватного та швидкого реагування на комп'ютерні надзвичайні події, а також важливим є подолання наслідків кібератак, що приходяться на критично важливу, акцентуємо на цьому увагу, інформаційну інфраструктуру. Натомість було створено відповідний спеціалізований підрозділ – CERT-UA – це команда, що має реагувати на комп'ютерні надзвичайні події в Україні, що виглядають як спеціалізований структурний підрозділ Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. Він має на меті допомогти усувати загрози щодо безпеки як приватного сектору України та можливих загроз іноземним партнерам. У відповідності до закону «Про основні засади забезпечення кібербезпеки України», що було прийнято у 2017 році, CERT-UA та Центр реагування на кіберзлочини повинні координувати заходи тактичного та оперативного реагування на кібератаки, окрім цього контролювати та впроваджувати контрзаходи, що мають передбачати мінімізацію вразливості всім системам зв'язку. Наша держава активно бере участь у роботі Агентства ЄС з кібербезпеки, а також Європейського центру, що займається дослідженнями і компетенціями в сфері кібербезпеки, окрім цього навчаються реалізовувати Спільну оперативну схему реагування ЄС і держав-членів на кібератаки.

Як не крути, але головними гравцями на світовій арені інформаційних технологій у відповідності до Індексу розвитку ІКТ (IDI) та Індексу мережевої готовності (NRI) у 2019 році є саме країни Південно-Східної Азії (Сінгапур і Японія), а також європейські країни (Фінляндія, Швеція, Норвегія, Нідерланди, Швейцарія, Велика Британія), не забуваючи про США. Адже їх економікам притаманно економічне зростання та високий рівень цифрового розвитку. Україна ж за Індексом розвитку ІКТ (ICT Development Index), у відповідності до Звіту Міжнародного союзу електрозв'язку

«Вимірювання інформаційного суспільства 2019» посідає 79 місце зі 176 країн, а беручи до уваги Індекс мережевої готовності (NRI) – 64 місце. Виходячи з цього, однією із основних причин невисокого місця України в вище зазначених рейтингах є, перш за все, саме нерівномірність в розвитку та нерівномірне впровадження ІКТ в різного роду сферах господарювання, а також різних регіонах. Припускаємо, що забезпечити безпеку в кіберпросторі є одним з факторів підвищення рівня цифрового розвитку в Україні.

Проведений аналіз показав, що високий рівень тісноти зв’язку (за шкалою Чеддока) між такими вище зазначеними показниками із значенням множинного коефіцієнта кореляції 0,7469. Водночас, R-квадрат та дана величина менше 0,6, що має вказувати на те, що точність апроксимації недостатня і дана модель буду вимагати введення нових незалежних змінних. Отже, можна сміливо Стверджувати, що підвищенням рівня кібербезпеки не буде постійно вистачати для того, щоб забезпечити розвиток цифрової економіки. Якщо ж ми згрупуємо країни саме за рівнем розвитку, то ми можемо побачити, що в розвинених країнах рівень кібербезпеки, а також рівень цифрового розвитку буде на порядок вищим, ніж в країнах, що розвиваються. В той же час, країни, що розвиваються продемонстрували, що можуть підвищити рівня кібербезпеки під впливом розвитку цифрової економіки, натомість відносно перших такий взаємозв'язок буде дещо слабшим.

ВИСНОВКИ

Розвитком цифрової економіки ми унеможливлюємо посилення кібербезпеки як на рівні в цілому держави, так і на рівні окремо взятих суб'єктів. Виходячи з цього, усвідомлення державою і бізнесом кібернетичних загроз, а також їх наслідків поки ще не набуває достатнього рівня важливості, та часто може сприйматися як дещо другорядне. Проте, результатами аналізу ми підкреслюємо, що існує деякий дуже тісний зв'язок, що проходить між рівнями кібербезпеки та цифрового розвитку, а саме: підвищення першої може неминуче призвести до прискорення другого і, в підсумку, підвищити добробут. Саме тому кібербезпека має посісти своє вагоме місце у загальній стратегії розвитку держави, а також кожної окремо взятої конкретної компанії. Отже, необхідним фактором є розробка окремої стратегії, а також програм безпеки, стосовно усієї бізнесекосистеми країни і державного управління в цілому. Держава має спільно з бізнесом докладати всіх можливих зусиль для того, щоб розробити та впровадити дієві системи кібербезпеки державного і корпоративного управління, а також провести наукові дослідження, щодо розробки конкретних засобів кіберзахисту в правовому, організаційному і технічному полях, розпочинаючи інформаційні та навчальні дії та кампанії стосовно підвищення в рівні обізнаності та навичок у сфері кібербезпеки, як для державних службовців, так і персоналу компаній, а також рядових громадян. В той же час, необхідно врахувати, що просто підвищення рівня кібербезпеки не може вирішити всіх та не може забезпечити сталий розвиток цифрової економіки, адже він напряму залежить від інших причин та факторів, можемо перерахувати: загальний рівень економічного, а також технологічного та соціального розвитку країни, рівня її положення у світовій економіці, також ефективності державного управління. Останній пункт має бути основним у адекватному формуванні державної стратегії кібербезпеки та дати ривок для подальшого розвитку цифрової економіки, адже усі без виключення кіберзлочини напряму пов'язані із несанкціонованим перерозподілом цих прав. Зазначимо, що для

нашої держави захист цих прав може становити проблему, виходячи з цього держава у силу її певних інституційних особливостей, сама може досить часто (в особі своїх дуже корумпованих представників в органах державного управління, а також правоохоронній і в судовій системах відповідно) виступати основним порушником цих прав як по відношенню до бізнесу, так і звичайних громадян, а кіберзлочинці дуже часто можуть ставати лише інструментом в руках корумпованих представників влади у незаконному перерозподілі власності, як правило шляхом використання сучасних інформаційно-комунікаційні технологій.

В першому розділі ми провели аналіз теоретичних засад поняття кібербезпеки, визначили основні критерії даного поняття, проаналізували основні тенденції його розвитку, а також різні підхід до його визначення.

В другому розділі нами були розглянуті основні методи дослідження кібербезпекової політики, описані їх основні складові, визначені переваги і недоліки різних методів оцінки.

Третій розділ було присвячено практичній оцінці проблематики кібербезпеки в Україні. Проведений аналіз показав, що високий рівень тісноти зв’язку (за шкалою Чеддока) між такими вище зазначеними показниками із значенням множинного коефіцієнта кореляції.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. О. Трофименко, "Моніторинг стану кібербезпеки в Україні", Правове життя сучасної України: матер. міжнар. наук.-практ. конф., 17 травня 2019 р., Т. 1, Одеса: Видавничий дім «Гельветика», с. 642–646, 2019.
2. National Strategies. [Електронний ресурс]. Режим доступу: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx.
3. Впровадження європейської кібербезпеки: загальний огляд. ISACA. [Електронний ресурс]. Режим доступу: https://www.isaca.org/Knowledge-Center/Research/Documents/European-CybersecurityImplementation-Overview_res_Ukr_1215.pdf
4. Державне агентство з електронного врядування України. [Електронний ресурс]. Режим доступу: https://www.e.gov.ua/ua.
5. Завдання Держспецзв’язку. [Електронний ресурс]. Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89831&cat_id=89828.
6. А. Задерейко, А. Троянський, Н. Логинова, Е. Трофименко, "Проблемные аспекты защиты информационного суверенитета Украины", Інфокомунікації – сучасність та майбутнє: матер. 7 міжнар. наук.-пр. конф., Одеса, 26–27 жовтня 2017 р., Т. 1, Одеса: ОНАЗ, С. 106–108.
7. Про основні засади забезпечення кібербезпеки України: Закон України. Урядовий кур'єр, № 215, 2017.
8. Баранов О. А. Інтернет речей: теоретикометодологічні основи правового регулювання / О. А. Баранов. – Київ, 2018. – Т. 1: Сфери застосування, ризики і бар'єри, проблеми правового регулювання. – 342 с
9. Ліпкан В.А., Дімчогло М.І. Консолідація інформаційного законодавства України: монографія; за заг. ред. В.А. Ліпкана. Київ: О.С.Ліпкан, 2014. 416 с

10. 10. Цимбалюк В.С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства. Київ : Освіта України, 2011. 426 с

11. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : монографія. / С. Ф. Гончар. – Київ, 2019. – 175 с

12. Грановський М. В. Державна політика у сфері запобігання та протидії кібернетичним загрозам – досвід Республіки Польща / М. В. Грановський // Теорія та практика державного управління. – 2019. – Вип. 4. – С. 212–220.

13. Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія. / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька. – Житомир, 2019. – 279 с.

14. Дудикевич В. Б. Квінтесенція інформаційної безпеки кіберфізичної системи. / В. Б. Дудикевич, Г. В. Микитин, А. І. Ребець // Вісник Національного університету «Львівська політехніка». – Інформаційні системи та мережі. – 2018. – № 887. – С. 58– 68.

15. Ткаченко О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. / О. Ткаченко, К. Ткаченко. // Цифрова платформа: інформаційні технології в соціо-культурній сфері. – 2018. – Вип. 1. – С. 75–86.

16. Яковів І. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека / І. Яковів // Information Technology and Security. – 2017. – Vol. 5. – № 2. – С. 134–144.

17. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. ... канд. юрид. наук : 12.00.01. Київ, 2007. 20 с.

18. Дяченко А. В., Карінцева О. І., Тарасенко С. В., Харченко М. О., Мазін Ю. О., Кисельова К. С. Формування інноваційного інструментарію економічної політики в умовах розвитку світової економічної кризи 2019-

2020 рр. в Україні // Механізм регулювання економіки. 2021. № 3. С. 19-37. https://essuir.sumdu.edu.ua/handle/123456789/86419

19. Економіка енергетики : підручник / за ред. Л. Г. Мельника, І. М. Сотник. – Суми: Університетська книга, 2015. – 378 с. https://essuir.sumdu.edu.ua/handle/123456789/45315

20. Економіка підприємства : підручник / за заг. ред. д.е.н., проф. Л. Г. Мельника. - Суми : Університетська книга, 2012. - 864 с. https://essuir.sumdu.edu.ua/handle/123456789/80106

21. Дяченко А. В., Карінцева О. І., Тарасенко С. В., Харченко М. О., Мазін Ю. О., Кисильова К. С. Формування інноваційного інструментарію економічної політики в умовах розвитку світової економічної кризи 2019-2020 рр. в Україні. Механізм регулювання економіки. 2021. № 3. С. 21-40. https://essuir.sumdu.edu.ua/handle/123456789/85737

22. Карінцева, О. І., Харченко, М. О., Мазін, Ю. О., Фалько, К. С. Практичні засади підвищення ефективності логістичної діяльності сучасного підприємства. Вісник Сумського державного університету. Серія Економіка. 2021. № 3. С. 127−136. DOI: 10.21272/1817-9215.2021.3-14 https://essuir.sumdu.edu.ua/handle/123456789/86223

23. Карінцева О.І., Дегтярьова І. Б., Харченко М.О., Долгошеєва О. І., Кіріл'єва А. В. Залучення іноземних інвестицій як інструмент забезпечення конкурентоспроможності та сталого розвитку країни. Вісник СумДУ. Серія «Економіка», № 3' 2020. С. 199-211. DOI: 10.21272/1817-9215.2020.3-22 https://visnyk.fem.sumdu.edu.ua/issues/3_2020/22.pdf

24. Карінцева, О. І., Харченко, М. О., Пономарьова, Г. С. Підвищення ефективності бізнес-процесів на виробничому підприємстві // Механізм регулювання економіки. 2020. № 4. С. 58-69. https://essuir.sumdu.edu.ua/handle/123456789/83754

25. Мельник Л. Г., Карінцева О. І. (2021) Економіка і бізнес : підручник / за ред. Л. Г. Мельника, О. І. Карінцевої. Суми : Університетська книга, 2021. 316 с. https://essuir.sumdu.edu.ua/handle/123456789/83721

26. Мельник Л. (2021) Сучасні тренди економічного розвитку: Досвід ЄС та практика України: підручник / за ред. Л. Г. Мельника. Суми: ПФ «Видавництво “Університетська книга”», 2021. 432 с. https://essuir.sumdu.edu.ua/handle/123456789/89235

27. Мельник Л. Г., Карінцева О. І., Кубатко О. В., Сотник І. М., Завдов’єва Ю. М. Цифровізація економічних систем та людський капітал: підприємство, регіон, народне господарство // Механізм регулювання економіки. 2020. № 2. С. 9-28. DOI: https://essuir.sumdu.edu.ua/handle/123456789/82236

28. Мельник, Л., Карінцева, О., Кубатко, О., Дерев’янко, Ю., Маценко, О. (2022). Реструктуризація соціально-економічних систем як складова формування цифрової економіки в Україні у період кризи. Механізм регулювання економіки, (1-2(95-96), 7-13.

29. Мельник, Л., Ковальов, Б. (2020). Проривні технології в економіці і бізнесі (Досвід ЄС та практика України у світлі III, IV, і V промислових революцій. Сумський державний університет, с. 180. https://essuir.sumdu.edu.ua/handle/123456789/79621

30. Сотник І. (2018) Підприємництво, торгівля та біржова діяльність / І. Сотник, Л. Таранюк. – Суми: Університетська книга, 2018. – 572 с. https://essuir.sumdu.edu.ua/handle/123456789/80114

31. Экономика развития: учебное пособие / под ред. д.-ра экон. наук, проф. Л. Г. Мельника, канд. экон. наук А. Вик. Кубатко. Сумы : «Университетская книга», 2017. 352 с. https://essuir.sumdu.edu.ua/handle/123456789/80184

32. Disruptive technologies for green economy formation in conditions of the fourth industrial revolution: the EU experience / I. Dehtyarova etc. // Socio-economic and management concepts: collective monograph / Krupelnytska I., – etc. – International Science Group. – Boston : Primedia eLaunch, 2021. P. 388-392. https://essuir.sumdu.edu.ua/handle/123456789/86986

33. Karintseva O., Kharchenko M., Boon E.K., ...Melnyk V., Kobzar O.(2021). Environmental determinants of energy-efficient transformation of national economies for sustainable development.. J. International Journal of Global Energy Issues, 2021, 43(2-3), P. 262–274 https://doi.org/10.1504/IJGEI.2021.115148

34. Karintseva O. I., Yevdokymov A. V., Yevdokymova A. V., Kharchenko M. O., Dron V. V. Designing the Information Educational Environment of the Studying Course for the Educational Process Management Using Cloud Services. Механізм регулювання економіки. 2020. № 3. С. 87-97. DOI: https://doi.org/10.21272/mer.2020.89.07 https://essuir.sumdu.edu.ua/handle/123456789/81759

35. Kubatko, O. V., Chortok, Y. V., Honcharenko, O. S., Nechyporenko, R. M., & Moskalenko, I. M. (2019). Studying Features of Vehicle Type Selection by Trade and Logistics Enterprise. Mechanism of economic regulation. – 2019. – №3. – С. 73–82. http://essuir.sumdu.edu.ua/handle/123456789/76448

36. Melnyk L., Sommer H., Kubatko O., Rabe M., Fedyna S. (2020). The economic and social drivers of renewable energy development in OECD countries. Problems and Perspectives in Management,18(4), 37-48. doi:10.21511/ppm.18(4).2020.04 https://essuir.sumdu.edu.ua/handle/123456789/82719

37. Melnyk L. H., Derykolenko O. M., Mazin Yu. O., Matsenko O. I., Piven V. S. Modern Trends in the Development of Renewable Energy: the Experience of the EU and Leading Countries of the World // Механізм регулювання економіки. 2020. № 3. С. 117-133. https://essuir.sumdu.edu.ua/handle/123456789/81810

38. Melnyk, L., Dehtyarova, I., Kubatko, O., Karintseva, O., & Derykolenko, A. (2019). Disruptive technologies for the transition of digital economies towards sustainability. Economic Annals-XXI, 179(9-10), 22-30. doi: https://essuir.sumdu.edu.ua/handle/123456789/85476

39. Melnyk, L., Dehtyarova, I., Karintseva, O., Kubatko, O. Information factors in economic systems and business during transition to digital

economy/Selected Aspects of Digital Society Development. Monograph 45. Edited by Tetyana Nestorenko and Aleksander Ostenda, Publishing House of University of Technology, Katowice, 2021. P. 173-178 https://essuir.sumdu.edu.ua/handle/123456789/87135

40. Melnyk, L., Matsenko, O., Dehtyarova, I. & Derykolenko, O. (2019). The formation of the digital society: social and humanitarian aspects. *Digital economy and digital society*. T. Nestorenko& M. Wierzbik-Strońska (Ed.). Katowice: Katowice School of Technology. [in Ukrainian].URL: http://essuir.sumdu.edu.ua/handle/123456789/74570

41. Melnyk L.G., Kubatko O. (2017) The impact of green-innovations on environmental quality and energy resource consumption. International economic relations and sustainable development : monograph / edited by Dr. of Economics, Prof. O. Prokopenko, Ph.D in Economics T. Kurbatova. – RudaŚląska :Drukarnia i Studio GraficzneOmnidiumю 272 p. ISBN 978-83-61429-11-1

42. The effects of the management of natural energy resources in the European Union / V. Voronenko, B. Kovalov, D. Horobchenko, P. Hrycenko // Journal of Environmental Management and Tourism. – Craiova: ASERS Publishing, 2017. – Vol. 8, Issue Number 7(23), P. 1410-1419. Available at: https://journals.aserspublishing.eu/jemt/article/view/1777

43. Tu Yu-Xia, Kubatko O., Karintseva O., Piven V. (2021) Decarbonisation drivers and climate change concerns of developed economies. International Journal of Environment and Pollution. 2021. 69 (1-2), 112-129

44. Veklych O., Karintseva O., Yevdokymov A., Guillamon-Saorin E.(2020). Compensation mechanism for damage from ecosystem services deterioration: Constitutive characteristic. J. International Journal of Global Environmental Issues, 19(1-3), P. 129–142 https://doi.org/10.1504/IJGENVI.2020.114869