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

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувачка випускової кафедри
_____Ніна РЖЕВСЬКА
«___»_____ 2022 р.

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

Тема: «ІНФОРМАЦІЙНА БЕЗПЕКА США ТА КНР В УМОВАХ ГЛОБАЛЬНОГО ПРОТИСТОЯННЯ»

Виконавець: здобувачка вищої освіти 4 курсу, 409 Б групи, Сидоркевич Анастасія Дмитрівна

Керівник: к.політ.н., доцент кафедри міжнародних відносин, інформації та регіональних студій, Алієв Максим Михайлович

Нормоконтролер _____ Валентина ЄМЕЦЬ
(підпис)

КИЇВ 2022

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Розвиток сучасного суспільства багато в чому ґрунтується на використанні інформаційних ресурсів. Інформація перестала бути лише одним із факторів виробництва, а управління інформацією не є більш прерогативою лише корпоративних структур. Інформація виступає також особливим громадським активом, причому його особливістю слід вважати формування одночасних позицій представників суспільства як споживачів інформації та як учасників її створення. Розвитку ролі інформації у суспільстві сприяє не лише створення нових засобів зв'язку та алгоритмів обробки інформації, втілених у програмні продукти. Основною рушійною силою зростання значимості інформації для суспільства та економіки слід вважати зміну ставлення до неї.

Сьогодні інформація стає інструментом, що одночасно визначає умови суспільного розвитку. Водночас розвиток інформаційного суспільства призводить і до зростання загроз національній та міжнародній безпеці, пов'язаних з порушенням встановлених режимів використання інформаційних та комунікаційних систем, утиском конституційних прав і свобод громадян, поширенням шкідливих програм, а також з використанням можливостей сучасних інформаційних технологій для здійснення ворожих, терористичних та інших злочинних дій. У зв'язку з цим особливу гостроту сьогодні набуває проблема забезпечення інформаційної безпеки, і насамперед надійного захисту інформації.

В даний час концепції інформаційної безпеки створені на державному рівні у багатьох країнах світу. Причина досить очевидна, пов'язана з практичними потребами запобігання негативним наслідкам впливу на економічну та суспільну інфраструктуру шкідливого програмного забезпечення (ПЗ), а також інших факторів, що створюють загрози для розвитку інформаційної сфери суспільства.

Інформаційна безпека (ІБ) – це стратегічний інструмент для створення та розповсюдження всілякої інформації, він став новим двигуном зростання економіки, новою платформою соціального управління, новим способом міжнародного співробітництва, до того ж абсолютно новою областю державного суверенітету.

Однак, ІБ надає нам не тільки ресурси, можливості, а й торкається низки питань. ІБ сучасної держави має прямий вплив на всі складові її політики. Голова КНР Сі Цзіньпін зазначив, що в наш час національна безпека неможлива без її кібербезпеки, а модернізація країни неможлива без її інформатизації.

З дедалі більшою роллю інформатизації у міжнародній політиці, зростають і ризики, пов'язані з бажаннями різних і державних, і недержавних акторів, порушити стабільність чи зовсім зруйнувати інформаційні структури інших держав.

На сьогоднішній день формування власного підходу до забезпечення інформаційної безпеки є необхідним для будь-якої держави. Таким чином, розвиток нового типу протистояння, як інформаційна боротьба, перехід гонки в технічних озброєннях в кіберпростір також зумовлюють актуальність дослідження відносин країн ІБ.

Одним із ключових факторів, що впливають на перебіг розвитку відносин у цій галузі, є відсутність у Пекіна та Вашингтона єдиного погляду на формування міжнародних норм регулювання кіберпростору, а також відсутність загального визначення «інформаційної безпеки». Ескалація китайсько-американських суперечок у питаннях ІБ стимулює зростання напруженості в кіберпросторі в цілому та провокує подальше втягування в гонку інформаційної безпеки усієї світової спільноти. Від кооперації чи суперництва навіть Китаю у цій сфері також залежить ІБ країн, які мають менш значними можливостями даному просторі.

У силу цих причин необхідно звернути увагу на американський і китайський підходи до формування політики в галузі ІБ, адже саме США та КНР вважаються одними з найвпливовіших акторів світової політики, а їх взаємодія в питаннях ІБ та стабільність системи взаємовідносин, що формується ними, мають глобальне значення.

Мета роботи – визначити сутність та особливості поняття інформаційної безпеки держав, їх проблеми та перспективи в умовах конфліктної взаємодії США та КНР.

Для реалізації мети необхідно вирішити **завдання:**

1. Визначити передумови формування поняття «інформаційна безпека».

2. Виявити теоретичні підходи до формування поняття «інформаційна безпека».

3. Розкрити методи та інструменти захисту інформаційної безпеки держав світу.

4. Встановити цілі та задачі США та КНР на міжнародній арені.

5. На основі комплексного аналізу офіційних документів виявити особливості нормативно-правових баз, що регулюють діяльність у просторі ІБ США та КНР;

6. Визначити наявні проблеми американо-китайських відносин у кіберпросторі та охарактеризувати основні події, що вплинули на формування цих проблем;

7. Розкрити стратегію інформаційної безпеки США КНР на сучасному етапі та в умовах конфліктної взаємодії.

Об'єкт дослідження – інформаційна безпека у сучасних міжнародних відносинах.

Предметом дослідження є інформаційна безпека США та КНР в умовах глобального протистояння.

Методологічна основа дослідження. Методологія дослідження зумовлена станом вивченості цієї теми та заснована на міждисциплінарному підході. Метод порівняльного аналізу був застосований до нормативно-правової бази США та КНР у сфері ІБ та дозволив виявити особливості забезпечення ІБ у досліджуваних країнах, позначити їх спільні інтереси. Історичний метод був використаний задля виявлення передумов виникнення поняття «інформаційна безпека» та його розвитку. Системний метод дозволив комплексно підійти до розуміння проблем ІБ відносно держав та їх перспектив на міжнародному рівні та аналізі розвитку інституційного аспекту забезпечення ІБ у Китаї та США.

Структурно кваліфікаційна робота складається зі вступу, трьох розділів, висновків і списку використаних інформаційних джерел (73 позиції).

РОЗДІЛ 1. СУТНІСТЬ ТА ОСОБЛИВОСТІ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Передумови формування поняття «інформаційна безпека»

Категорія «інформаційна безпека» виникла з появою засобів інформаційних комунікацій, а також усвідомленням наявності у людей та їх угруповань інтересів, яким може бути завдано шкоди шляхом впливу на засоби інформаційних комунікацій, наявність та розвиток яких забезпечує інформаційний обмін між усіма елементами соціуму.

У розвитку засобів інформаційних комунікацій можна назвати кілька етапів:

І етап – до початку XIX століття. У цей період основним завданням інформаційної безпеки був захист відомостей про події, факти, майно, місцезнаходження й інші дані, що мали для людини особисто або соціуму, до якого вона належала, життєве значення. В широкому сенсі заходи захисту інформації було спрямовано на запобігання перехопленню фізичних повідомлень, особливо під час ведення бойових дій.

З перших днів спілкування дипломати та військові командири розуміли, що необхідно забезпечити певний механізм захисту конфіденційності кореспонденції та мати певні засоби виявлення фальсифікацій. Юлію Цезарю приписують винахід шифру Цезаря бл. 50 до н.е., який був створений для того, щоб запобігти читанню його таємних повідомлень, якщо повідомлення потрапить у чужі руки. Однак здебільшого захист був досягнутий за допомогою застосування процедурних засобів контролю. Конфіденційна інформація була позначена, щоб вказати, що її слід захищати та транспортувати довіреними особами, охороняти та зберігати в захищеному середовищі або надійному ящику. У міру розширення поштових послуг уряди створювали офіційні організації для перехоплення, розшифровки, читання та повторного запечатування листів (наприклад, Секретне бюро Великобританії, засноване в 1653 році).

II етап – починаючи з 1816 року – пов'язаний з появою та використанням технічних засобів електро- та радіозв'язку. Для забезпечення скритності і перешкодно-захищеності радіозв'язку необхідно було використовувати досвід першого періоду інформаційної безпеки на більш високому рівні розвитку, а саме застосування завадостійкого кодування повідомлення з подальшим декодуванням прийнятого повідомлення.

У середині XIX століття були розроблені більш складні системи класифікації, щоб дозволити урядам керувати своєю інформацією відповідно до ступеня чутливості. Наприклад, британський уряд певною мірою кодифікував це з опублікуванням Закону про офіційну таємницю в 1889 році. Розділ 1 закону стосувався шпигунства та незаконного розкриття інформації. Незабаром було додано захист суспільних інтересів, щоб захистити розкриття інформації в інтересах держави. Подібний закон був прийнятий в Індії в 1889 році, Закон про офіційну таємницю Індії, який був пов’язаний з британською колоніальною епохою і використовувався для боротьби з газетами, які виступали проти політики Раджа. На час Першої світової війни багаторівневі системи класифікації використовувалися для передачі інформації на різні фронти та з них, що спонукало до більш широкого використання розділів для створення кодів і розриву в дипломатичних і військових штабах. Між війнами кодування стало більш складним, оскільки машини використовувалися для скремблування та розшифровки інформації.

III етап – починаючи з 1935 року – поява радіолокаційних та гідроакустичних засобів. Основним способом забезпечення інформації було поєднання організаційних та технічних заходів, спрямованих на підвищення захищеності радіолокаційних засобів від впливу на їх приймальні пристрої активними маскуючими та пасивними радіоелектронними перешкодами, що імітують.

Встановлення комп’ютерної безпеки започаткувало історію інформаційної безпеки. Потреба в цьому виникла під час Другої світової війни. Обсяг інформації, яку поширювали країни Альянсу під час Другої світової війни, вимагав формального узгодження систем класифікації та процедурного контролю. Розвинувся таємничий діапазон маркувань, які вказували на те, хто може працювати з документами

(зазвичай офіцери, а не рядові війська) і де їх слід зберігати, оскільки створювалися дедалі складніші сейфи та сховища. Машина Enigma, яку німці використовували для шифрування даних війни та була успішно розшифрована Аланом Тьюрингом, можна розглядати як яскравий приклад створення та використання захищеної інформації. Процедури еволюціонували для забезпечення належного знищення документів, і саме недотримання цих процедур призвело до деяких з найбільших розвідувальних переворотів війни (наприклад, захоплення U-570).

IV етап – починаючи з 1946 року – винахід та впровадження у практичну діяльність електронно-обчислювальних машин. Завдання інформаційної безпеки вирішувалися, переважно, обмеженням фізичного доступу до устаткування засобів добування, переробки та передачі.

Різні мейнфрейми були підключені до Інтернету під час холодної війни для виконання складніших завдань, у процесі комунікації легше, ніж розсилання магнітних стрічок назад і вперед комп'ютерними центрами. Таким чином, Агентство перспективних дослідницьких проектів (ARPA) Міністерства оборони США розпочало дослідження доцільності створення мережевої системи зв'язку для торгівлі інформацією в Збройних Силах Сполучених Штатів.

V етап – починаючи з 1965 року – створення та розвиток локальних інформаційно-комунікаційних мереж. Завдання інформаційної безпеки також вирішувалися, методами та способами фізичного захисту засобів добування, переробки та передачі інформації, об'єднаних у локальну мережу шляхом адміністрування та управління доступом до мережевих ресурсів. У 1968 році доктором Ларрі Робертсом був розроблений проект ARPANET, який згодом перетворився на те, що відоме як Інтернет.

VI етап – починаючи з 1973 року – використання надмобільних комунікаційних пристроїв з широким спектром завдань. Для забезпечення інформаційної безпеки в комп'ютерних системах з бездротовими мережами передачі даних була потрібна розробка нових критеріїв безпеки. Утворилися спільноти хакерів, які ставлять собі за мету завдати шкоди інформаційній безпеці окремих користувачів, організацій та цілих країн. Інформаційний ресурс став найважливішим ресурсом держави, а

забезпечення її безпеки – найважливішої та обов'язкової складової національної безпеки. Формується інформаційне право – нова галузь міжнародної правової системи.

VII етап – від 1985 року. Створення та розвиток глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення. Всеосяжна автоматизація виробничих процесів на підприємствах також вимагає розширення заходів інформаційної безпеки, що потребує постійного оновлення політики безпеки [26].

Кінець XX та перші роки XXI століття ознаменувалися швидким прогресом у сфері телекомунікацій, комп'ютерного обладнання та програмного забезпечення та шифрування даних. Наявність меншого, потужнішого та менш дорогого обчислювального обладнання зробило електронну обробку даних доступною для малого бізнесу та домашніх користувачів. Запровадження протоколу керування передачею/протоколу мережі (TCP/IP) на початку 1980 років дозволило різним типам комп’ютерів спілкуватися. Ці комп’ютери швидко з’єдналися через Інтернет.

На сучасному етапі з бурхливим розвитком інформаційних технологій і їх широким впровадженням в облікові процеси виникає проблема взаємодії цих облікових систем з іншими системами та між собою, а також проблема конфіденційності. До того ж, ці проблеми існують на технічному, програмному та інформаційному рівнях. Вирішити їх можна шляхом розроблення і впровадження єдиних, загальних і обов'язкових правил побудови і використання облікових інформаційних систем. У світлі розвитку нових IT-технологій, поняття інформаційної безпеки значно розширилося. Сьогодні від захисту процесів, інформації та діяльності в кіберпросторі залежить значно більше, ніж просто втрата інформації. Тобто, втрата інформації тягне за собою низку інших комплексних ускладнень. Нині комплекс заходів із захисту інформації повинен враховувати, в тому числі, антивірусний захист, захист від хакерських атак, підробки даних тощо. Наприклад, враження комп’ютерними вірусами може не лише видалити чи викрасти дані, але й вплинути на роботу та продуктивність співробітників чи навіть зупинити виробництво.

Швидке зростання та широке використання електронної обробки даних та електронного бізнесу, що ведеться через Інтернет, разом із численними явищами міжнародного тероризму підігрівають потребу в кращих методах захисту комп’ютерів та інформації, яку вони зберігають, обробляють та передають. Академічні дисципліни комп'ютерної безпеки та забезпечення інформації з'явилися разом з численними професійними організаціями, які поділяють спільні цілі забезпечення безпеки та надійності інформаційних систем .

1.2 Теоретичні підходи до формування поняття «інформаційна безпека»

Інформаційна безпека існувала починаючи від паперових технологій та завершуючи програмно-технічними комплексами; вона стосується різних сфер діяльності та впроваджується з метою попередження втрат інформації та кіберзлочинності, а також порушення якої пов’язано із кримінальною відповідальністю.

Цілком очевидно, що, за відсутності чіткого розуміння інформаційної безпеки, зокрема, позначення меж, у яких політика ІБ має проводитися, неможливо й виробити по-справжньому ефективні заходи, які забезпечують відсутність загроз критичного на об'єкти інформаційної інфраструктури, і навіть життя суспільства. Поняття «інформаційна безпека» надзвичайно складне, а для його розуміння використовують різні наукові трактування.

Проблематика інформаційної безпеки складна і багатоаспектна, що зумовлює необхідність вивчення й узагальнення наукових праць представників різних галузей науки. Окремі аспекти регулювання інформаційної сфери стали об’єктом наукового аналізу в працях українських і зарубіжних дослідників.

Перший підхід – статичний, пов’язує інформаційну безпеку із станом захищеності, що не зовсім вірно, оскільки вона забезпечує його, використовуючи різні засоби. Тобто подібні визначення роблять акцент на мету функціонування інформаційної безпеки. Такого підходу дотримується О. Литвиненко. Під поняттям

ІБ розуміє єдність трьох складників: забезпечення захисту інформації; забезпечення захисту й контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності.

Другий підхід передбачає те, що інформаційна безпека є процесом, який включає застосування різного роду програмних, технічних, правових, інформаційних та організаційних інструментів для забезпечення функціонування її основної мети. Також некоректним буде вважати інформаційну безпеку тільки процесом, тобто послідовністю виконання дій щодо захисту, оскільки вона може передбачати реалізацію ряду взаємопов'язаних процесів, спрямованих на виявлення та попередження загроз.

Л. Харченко, В. Ліпкан, О. Логінов визначили, що інформаційна безпека – це складник національної безпеки, процес управління загрозами та небезпеками, державними й недержавними інституціями, окремими громадянами.

Третій підхід – комплексний, є досить широким, оскільки наголошує, що інформаційна безпека є мультидисциплінарною сферою. Хоча можна погодитися із тим, що вона є саме сферою діяльності, але такий підхід робить її тільки певним різновидом надання послуг.

Т. Ткачук в праці «Забезпечення інформаційної безпеки: досвід окремих країн східної Європи» обґрунтував авторську позицію, що найбільш прийнятним, зважаючи на сучасну практику забезпечення інформаційної безпеки держави, є останній (комплексний). За такого підходу вбачається за доцільне інформаційну безпеку держави розглядати як перманентний процес діяльності компетентних органів, спрямований на запобігання і протидію загрозам в інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час. Цей підхід базується на принципі, відповідно до якого основною метою забезпечення інформаційної безпеки є створення безпечного інформаційного середовища [39].

Л. Наливайко трактує інформаційну безпеку як сукупність засобів забезпечення інформаційного суверенітету, захист інформаційної сфери від зовнішніх і внутрішніх

інформаційних загроз. Ця безпека має включати ефективну протидію сукупності інформаційних загроз.

Як бачимо, поширення набули структурний підхід до розуміння поняття «інформаційна безпека», за яким воно розглядається в контексті національної безпеки як її складник; діяльнісний підхід, що дає змогу розглядати інформаційну безпеку як процес, функцію держави, діяльність органів державної влади; підхід, згідно з яким інформаційна безпека розглядається в статичному стані, як певний стан захищеності чи стан правових норм; підхід, що дає змогу розглядати інформаційну безпеку як суспільні відносини.

У теоретико-правових дослідженнях інформаційної безпеки доцільно її розглядати крізь призму правовідносин, що виникають під час забезпечення стану захищеності інформаційного простору. Отже, інформаційну безпеку можна визначити як правовідносини, що виникають під час здійснення превентивних і захисних заходів в інформаційному середовищі людини, суспільства та держави.

Оскільки наслідки інформаційних загроз, попередження яких є головною задачею інформаційної безпеки, є суттєвими для суспільства, то не погоджуємося із такими трактуваннями в повній мірі, оскільки вони знижують цінність інформаційної безпеки для суспільства.

Таблиця 1.1

Зміст підходу	Автор або джерело	Визначення інформаційної безпеки
Інформаційна безпека, як стан	ООН	Це «стан міжнародних відносин, що виключає порушення світової стабільності та створення загрози безпеці держав та світової спільноти в інформаційному просторі».
	Закон України «Про Основні засади розвитку інформаційного суспільства в Україні»	Це «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження,

		використання і порушення цілісності, конфіденційності та доступності інформації»
	Кормич Б.А.	Це «стан захищеності встановлених законодавством норм, параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини, суспільства як суб'єктів процесів та відносин»
Інформаційна безпека, як процес	ISO/IEC 27000	Це «збереження конфіденційності, цілісності та доступності інформації. Примітка. Крім того, можуть бути задіяні й інші властивості, такі як достовірність, підзвітність, відмова та надійність»
	SNSS	Це «захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації, знищення для забезпечення конфіденційності, цілісності та доступності»
	ISACA	Вона «забезпечує таким чином, що лише авторизовані користувачі (конфіденційність) мають доступ до точної та повної інформації (цілісність), коли це потрібно (наявність)»
	SANS Institute	Вона «відноситься до процесів та методологій, які розроблені та впроваджені для захисту друкованої, електронної чи будь-якої іншої форми, приватної та конфіденційної інформації, чи даних від несанкціонованого доступу, використання, розкриття, зловживання, знищення, модифікації чи порушення»
Інформаційна безпека, як сфера діяльності	Cherdantseva Y., Hilton J.	Це «мультидисциплінарна сфера вивчення та професійної діяльності, яка займається розробкою та впровадженням усіх доступних типів механізмів безпеки (технічних, організаційних, орієнтованих на людину, юридичних) з метою збереження інформації у всіх її місцях (усередині та поза периметром організації) і, отже, в інформаційних системах, де інформація створюється, обробляється, зберігається, передається та знищується, вільна від загроз»

Проаналізувавши нормативно-правові документи, було узагальнено підходи до визначення інформаційної безпеки з позиції властивостей функціонування та зазначено в таблиці 1.1:

1. Інформаційна безпека, як стан

Даного підходу дотримуються ООН та трактують ІБ, як «стан міжнародних відносин, що виключає порушення світової стабільності та створення загрози безпеці держав та світової спільноти в інформаційному просторі».

Закон України «Про Основні засади розвитку інформаційного суспільства в Україні» (№ 1-1/175903, 07.2012) зазначають, що це «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації».

Кормич Б.А., український науковець-правознавець, доктор юридичних наук також дотримується даного підходу та трактує: «ІБ – це стан захищеності встановлених законодавством норм, параметрів інформаційних процесів та відносин, що забезпечує необхідні умови існування держави, людини, суспільства як суб'єктів процесів та відносин».

Інформаційну безпеку, як стан також визначають такі вчені, як: В. Богуш, В.А. Ліпкан, В.А. Авраменко, Р. Калюжний, Н.Р. Нижник, Я.М. Жарков, В.Т. Білоус та О.І. Барановський.

2. Інформаційна безпека, як процес

Серія міжнародних стандартів ISO/IEC 27000: «Збереження конфіденційності, цілісності та доступності інформації. Примітка. Крім того, можуть бути задіяні й інші властивості, такі як достовірність, підзвітність, відмова та надійність».

SNSS: «Захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації, знищення для забезпечення конфіденційності, цілісності та доступності».

ISACA: «ІБ забезпечує таким чином, що лише авторизовані користувачі (конфіденційність) мають доступ до точної та повної інформації (цілісність), коли це потрібно (наявність)».

SANS Institute: «ІБ відноситься до процесів та методологій, які розроблені та впроваджені для захисту друкованої, електронної чи будь-якої іншої форми, приватної та конфіденційної інформації, чи даних від несанкціонованого доступу, використання, розкриття, зловживання, знищення, модифікації чи порушення».

3. Інформаційна безпека, як сфера діяльності

Доктори комп'ютерних наук та інформатики Кардіффського університету (Кардіфф, Великобританія) Cherdantseva Y., Hilton J. У своїй праці А «Reference Model of Information Assurance & Security», зазначають, що «ІБ – це мультидисциплінарна сфера вивчення та професійної діяльності, яка займається розробкою та впровадженням усіх доступних типів механізмів безпеки (технічних, організаційних, орієнтованих на людину, юридичних) з метою збереження інформації у всіх її місцях (усередині та поза периметром організації) і, отже, в інформаційних системах, де інформація створюється, обробляється, зберігається, передається та знищується, вільна від загроз» [73].

Слід відмітити, що вітчизняні науковці приділяють неабияку увагу вивченню різних аспектів інформаційної безпеки. Так, її правовий базис досліджували Б. Кормич [20], В. Петрик [32]; її психологічний вплив на окремих індивідів та державу в цілому – У. Ільницька [19]; її проблеми, вплив, наслідки та шляхи вирішення для суб'єктів підприємницької діяльності – Т. Микитенко, І. Петровська, П. Рогов, А. Гаркуша [28]; М. Зубок [18]; її формування як основа національної безпеки – І. Боднар [6]; її понятійний апарат – В. Остроухов, В. Петрик [31], та інші. Хоча питання інформаційної безпеки є досить актуальним та досліджується для різних сфер життєдіяльності суспільства, але в наукових публікаціях існує ряд невизначеностей, пов'язаних із відсутністю єдиних підходів до трактування її поняття, що впливає на подальше розуміння її сутності.

Інформаційна безпека є складним, системним, багаторівневим явищем, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні та внутрішні

чинники, найважливішими з яких є: 1) політична обстановка у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку країни; 4) внутрішньополітична обстановка в державі. Водночас інформаційна безпека є складною, динамічною, цілісною соціальною системою, компонентами якої є підсистеми безпеки особистості, держави і суспільства. Саме взаємозалежна, системна інформаційна єдність останніх складає якісну визначеність, покликану здійснити захист життєво важливих інтересів людини, суспільства і держави, забезпечити їх конкурентоздатний, прогресивний розвиток [17].

Проаналізувавши нормативно-правові документи, праці вітчизняних та зарубіжних науковців, варто виділити трактування Т. Ткачука, кандидата юридичних наук та автора публікації «Забезпечення інформаційної безпеки: досвід окремих країн східної Європи». Серед усіх джерел, визначення Т. Ткачука найбільше стосується даного дослідження.

Науковець обґрунтував авторську позицію, що найбільш прийнятним підходом, зважаючи на сучасну практику забезпечення інформаційної безпеки держави, є комплексний. За такого підходу вбачається за доцільне інформаційну безпеку держави розглядати як перманентний процес діяльності компетентних органів, спрямований на запобігання і протидію загрозам в інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час. Цей підхід базується на принципі, відповідно до якого основною метою забезпечення інформаційної безпеки є створення безпечного інформаційного середовища.

Виходячи із проведеного аналізу та синтезу отриманої інформації, узагальненої в таблиці, застосуємо системний підхід, який дозволить сформувати поняття інформаційної безпеки з урахуванням недоліків окремих підходів. З цією метою виділимо риси, характерні для більшості визначень інформаційної безпеки, та представимо їх у вигляді схеми.

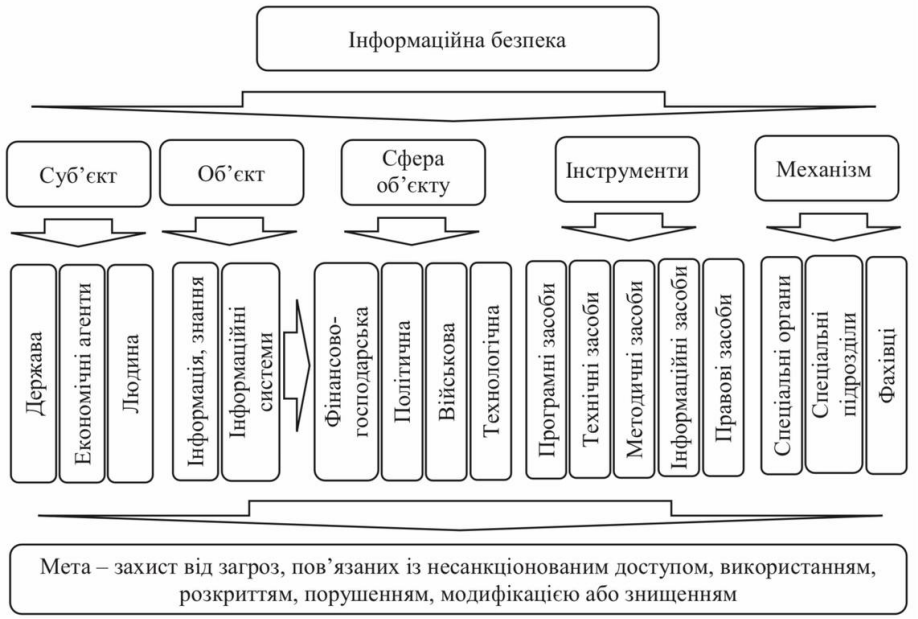

Рис.1.1 Риси інформаційної безпеки [34].

Тобто системний підхід передбачає розгляд та дослідження будь-яких систем з позиції мети їх функціонування, суб'єктів, які приймають участь у її забезпеченні, об'єктів, які функціонують у певній сфері діяльності, та на яких направлено інструменти впливу, а також механізмів, які забезпечують виконання та регулювання системи. Згідно із цим, на рисунку 1 представлені основні компоненти інформаційної безпеки, як системи, що дозволило сформулювати власне поняття інформаційної безпеки: інформаційна безпека – це комплексна система, мета функціонування якої – захист об'єктів (інформація, знання, інформаційні системи), що належать до фінансово-господарської, політичної, військової, технологічної сфер діяльності, від різного роду загроз (несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення) із застосуванням програмних, технічних, методичних, інформаційних та правових засобів, що використовують окремі особи або спеціалізовані підрозділи та фахівці державних органів, економічних агентів.

Важливою темою також є проблеми та загрози інформаційної безпеки. Достатньо згадати Іран 2010 року (реалізований проект за допомогою спеціально розробленого вірусу Stuxnet, який вивів з ладу майже 1000 центрифуг, призначених для збагачення урану), Венесуела березень 2019 року (витік інформації), Велика

Британія, Китай, США – це лише незначний перелік держав, які зазнали чи були ініціатором масштабних кібератак. Рівень інформаційної безпеки держави, значною мірою, зумовлений рівнем її інформаційної інфраструктури.

Основними завданнями системи ІБ є:

1. Своєчасне виявлення та усунення загроз безпеці та ресурсам, причин та умов, що сприяють завданню фінансової, матеріальної та моральної шкоди його інтересам;

2. Створення механізму та умов оперативного реагування на загрози безпеці та прояву негативних тенденцій у функціонуванні підприємства.

3. Ефективне припинення зазіхань на ресурси та загрози на основі правових, організаційних та інженерно-технічних заходів та засобів забезпечення безпеки.

4. Створення умов для максимально можливого відшкодування та локалізації шкоди, що завдається, неправомірними діями фізичних та юридичних осіб, послаблення негативного впливу наслідків порушення безпеки на досягнення цілей організації.

Як показує міжнародна практика, основна проблема у сфері забезпечення інформаційної безпеки полягає у створенні єдиного ефективного механізму, який дозволяв би своєчасно застосовувати на практиці нормативно-правові, законодавчі акти, що відповідають існуючим соціально-політичним та економічним умовам та досягненням у галузі інформаційних технологій. Розвиток технологій, сфери інформатизації робить актуальним питання забезпечення інформаційної безпеки.

Проблема забезпечення інформаційної безпеки має дві складові – технологічну та ідеологічну. Перша – пов'язана з розробкою та впровадженням інформаційних ресурсів, системи захисту інформаційних баз, друга – з поширенням інформації, її впливом на життя особистості, суспільства, держави.

Отже, наявність в літературі різних підходів до інформаційної безпеки свідчить про те, що інформаційна безпека, по-перше, є багатоаспектною і багатовимірною, по-друге, стосується всіх сфер суспільного життя, по-третє, пов’язана з урізноманітненням і збільшенням кількості потенційних загроз і дестабілізуючих чинників.

1.3 Методи та інструменти захисту інформаційної безпеки держав світу

Задля забезпечення цілісності, доступності та конфіденційності інформації необхідно захистити її від несанкціонованого доступу, руйнування, незаконного копіювання та розголошення. Забезпечення інформаційної безпеки – це комплекс організаційних та технічних заходів, спрямованих на захист даних.

До методів захисту інформації відносять засоби, заходи та практики, які мають захищати інформаційний простір від загроз – випадкових та зловмисних, зовнішніх та внутрішніх. Мета діяльності щодо забезпечення інформаційної безпеки – захистити дані, а також спрогнозувати, запобігти та пом'якшити наслідки будь-яких шкідливих впливів, які можуть завдати шкоди інформації (видалення, спотворення, копіювання, передача третім особам тощо). Відомі на сьогодні загальні методи забезпечення інформаційної безпеки складаються з організаційно-технічних, економічних та правових.

Організаційно-технічні методи інформаційної безпеки (ІБ) включають:

1. Систему забезпечення інформаційної безпеки (під нею ми маємо на увазі комплекс заходів (внутрішні правила роботи з даними, регламент передачі відомостей, доступ до них тощо) та технічних засобів (використання програм та приладів для збереження конфіденційності даних).

2. Розробку (створення нових), експлуатацію та вдосконалення вже наявних засобів захисту інформації.

3. Перманентний контроль за дієвістю вжитих заходів у сфері забезпечення інформаційної безпеки.

Останній пункт особливо важливий. Без методики оцінки дуже важко визначити ефективність ІБ. Якщо ефективність падає, необхідно терміново вносити корективи (для цього потрібна перманентність контролю).

Правовий фактор безпеки складається з:

1. Ліцензування діяльності щодо забезпечення інформаційної безпеки.

2. Сертифікації технічних засобів інформаційного захисту.

3. Атестації об'єктів інформатизації відповідно до відповідності норм інформаційної безпеки.

Організаційні методи захисту інформації включають заходи та дії, які повинні здійснювати посадові особи у процесі створення та експлуатації технологічних засобів для забезпечення заданого рівня безпеки інформації.

Організаційні методи захисту тісно пов'язані з правовим регулюванням у сфері безпеки інформації. Відповідно до законів та нормативних актів у міністерствах, відомствах, на підприємствах (незалежно від форм власності) для захисту інформації створюються спеціальні служби безпеки (на практиці вони можуть називатися й інакше). Ці служби підпорядковуються, зазвичай, керівництву установи. Керівники служб організують створення та функціонування систем захисту інформації. На організаційному рівні вирішуються такі завдання забезпечення безпеки інформації:

1. Організація робіт із розробки системи захисту інформації.
2. Обмеження доступу на об'єкт та до ресурсів КС.
3. Розмежування доступу до ресурсів КС.
4. Планування заходів.
5. Розробка документації.
6. Виховання та навчання обслуговуючого персоналу та користувачів.
7. Сертифікація засобів захисту.
8. Ліцензування діяльності із захисту інформації.
9. Атестація об'єктів захисту.
10. Вдосконалення системи захисту.
11. Оцінка ефективності функціонування системи захисту.
12. Контроль за виконанням встановлених правил роботи.

Організаційні методи є стрижнем комплексної системи захисту. Тільки за допомогою цих методів можливе об'єднання на правовій основі технічних, програмних та криптографічних засобів захисту в єдину комплексну систему. Конкретні організаційні методи захисту будуть наводитися під час розгляду відображення загроз безпеки інформації.

У своїй діяльності з розвитку та вдосконалення системи інформаційної безпеки державні органи переслідують такі цілі:

1. Зміцнення системи вертикального управління та централізація сил інформаційної безпеки на федеральному, міжрегіональному, регіональному та муніципальному рівнях, а також на рівні об'єктів інформатизації, операторів інформаційних систем та мереж зв'язку.

2. Вдосконалення форм та методів взаємодії сил інформаційної безпеки з метою підвищення їхньої готовності до протидії інформаційним загрозам, у тому числі шляхом проведення регулярних навчань.

3. Удосконалення інформаційно-аналітичних та науково-технічних аспектів функціонування системи інформаційної безпеки.

4. Підвищення ефективності взаємодії державних органів, органів місцевого самоврядування, організацій та громадян під час виконання завдань інформаційної безпеки.

Інформаційна безпека – це завжди комплексна система, всі складові якої покликані не допустити витоку конфіденційних відомостей технічних каналів, а також запобігти сторонньому доступу до носіїв інформації. Все це відповідно гарантує цілісність даних при роботі з ними: обробці, передачі та зберіганні, які повинні здійснюватися обов'язково в правовому полі. Грамотно організовані технічні заходи дозволяють визначити використання спеціальних електронних пристроїв несанкціонованого зняття інформації, розміщених як у приміщенні, і у засобах зв'язку.

1.4 Цілі та задачі США та КНР на міжнародній арені

Сполучені Штати Америки та Китайська Народна Республіка – головні геополітичні гравці та лідируючі військові держави. Відносини між КНР та США здавна мають складну природу та завжди включають дві складові: елементи співпраці та елементи конкуренції. Сьогодні американо-китайські відносини вважають одними

з найбільш важливих двосторонніх зв’язків наддержав. Кожна з яких має свої цілі та задачі на міжнародній арені.

США проводять складну зовнішню політику, основними принципами якої проголошено «будівництво безпечного світу» та «поширення демократії на благо американського народу та міжнародного співтовариства». Сполучені Штати відіграють важливу роль у міжнародних відносинах, мають найрозвиненішу у світі мережу дипломатичних представництв. США – член-засновник Організації Об'єднаних Націй та Північно-атлантичного альянсу, член Ради Безпеки ООН. Дипломатія США бере найактивнішу участь у вирішенні практично всіх міжнародних конфліктів та суперечок.

США, як глобальний лідер, мають свої інтереси у всіх регіонах світу та почуваються відповідальними за міжнародний порядок. Геополітична стратегія США набуває більш жорстких форм з метою обмежити їх активність і нейтралізувати їх ресурси, особливо якщо створення коаліції під американськими прапорами проблематично. Таким чином, залучаючи нових членів, США готують ґрунт для збереження над ними свого контролю.

Одним із напрямів у зовнішній політиці США є проведення політики «М'якої сили» (Soft power). Вона діє, спонукаючи інших слідувати (або домагаючись їхньої власної згоди слідувати, або роблячи вигідним дотримання) певним нормам поведінки та інститутам на міжнародній арені, що і призводить її носіїв до досягнення бажаного результату фактично без примусу». Політика «м'якої сили» – це непомітне поширення серед населення симпатії до Америки, почуття її переваги над своєю країною.

Проаналізувавши інтернет-ресурси (зокрема, сайт МЗС США https://www.state.gov/), наукову літературу («US Foreign Policy 3e» Edited by Michael Cox and Doug Stokes, «The American Way of Strategy: U.S. Foreign Policy and the American Way of Life» by Michael Lind) та нормативно-правові документи було узагальнено геополітичні цілі США:

1. Забезпечувати високий рівень бойової готовності американських збройних сил, щоб запобігати війні, демонструвати силу, а якщо стримування за допомогою залякування не дає результату, то застосовувати її на користь країни.

2. Заохочувати економічне зростання та політичну відкритість, поширюючи блага вільної торгівлі та стійкої міжнародної валютної системи на всі країни, віддані цим принципам, у тому числі й країни Західної півкулі.

3. Відродити міцні та тісні відносини з союзниками, які поділяють американські цінності і тому здатні розділити тягар зусиль заради миру, процвітання та свободи.

4. Вільний доступ до моря. США виступає за свободу доступу до морів і намагається реалізувати цю політику за допомогою військових баз у Японії, а також угодами про надання доступу на території із Сінгапуром та іншими Південно-Східними азіатськими країнами.

5. Наголосити на розвитку багатопланових відносин з великими державами, особливо Росією та Китаєм, які з часом зможуть визначати характер світової політичної системи.

6. Запобігання розповсюдженню зброї масового ураження та балістичних систем доставки ракет. Ці інтереси реалізуються за допомогою 6-ти сторонніх переговорів з Китаєм, Південною Кореєю, Японією, Росією та Північною Кореєю щодо роззброєння Північної Кореї. Водночас широкою підтримкою в регіоні користується Ініціатива з безпеки у боротьбі з поширенням зброї масового знищення (ІБОР-ОМУ).

7. Рішуче нейтралізувати загрозу з боку «держав-ізгоїв» та вороже настроєних держав, які нарощують потенціал терористичної діяльності та провадження зброї масового знищення.

Реалізація цих завдань багато в чому полегшується тим, що ніхто з порівнянних зі США за потужністю міжнародних суб'єктів-Японія, Китай та ЄС-поки не готовий взяти на себе функції одного з глобальних лідерів. Спроба забезпечити беззастережне підпорядкування інтересам Америки, зокрема західноєвропейських держав, дедалі частіше зустрічає опір. Така поведінка європейців харчується не лише конкуренцією

між ними на світових ринках, а й прагненням послабити політичний тиск США як на вибір орієнтирів зони дії НАТО, так і на орієнтири міжнародної політики ЄС загалом.

КНР. Упродовж останніх тридцяти років економіка Китаю розвивалася надзвичайно швидкими темпами. Китай довів здатність як ефективно планувати стратегічний розвиток країни, а й оптимально використовувати всі наявні ресурси зміцнення свого впливу у світі.

У сучасній міжнародній системі КНР стала центром сили, з якою не можна не рахуватися. У державах, що нині визначають світову політику, жоден діяч, який розробляє чи реалізує проекти в області безпеки надрегіонального значення, не може ігнорувати китайський фактор. Починаючи ще від 17 вересня 2002 р. в «Стратегії національної безпеки США» КНР віднесена до потенційно великої держави – недемократичної, але з ринковою економікою, за котрою визнається безперечне право володіти й удосконалювати ракетні та ядерні військові технології. Контури світу, в якому Китай відіграватиме роль геополітичного і геостратегічного центру, поки що складно окреслити, але він поступово формується, незалежно від бажання тих чи інших міжнародних акторів.

На основі аналізу інтернет-ресурсів, наукової літератури та, зокрема, першого джерела «Military and security developments involving the People’s Republic of China 2021» (Annual Report to Congress by Office of the Secretary of Defense) було визначено наступні стретегічні регіональні цілі, які Китай в даний час досягає [58]:

1. Визнання світовою спільнотою територіальної цілісності Китаю, включаючи його права на Тайвань, Тибет, Сіньцзян.
2. Забезпечення сприятливої міжнародної обстановки для розвитку та модернізації КНР.
3. Диверсифікація доступу Китаю до енергетичних ресурсів.
4. Запобігання спробам стримувати зростання потужності КНР.
5. Міжнародне визнання «особливих» прав КНР на акваторію Південно-Китайського моря (де перетинаються нафтові інтереси дев'яти її сусідів та регіону).
6. Поширення переважаючого впливу на Південно-Східну Азію.

7. Прийнятне для Китаю вирішення територіальних питань із сусідніми державами (тут йдеться насамперед про Індію, відносини з якою, незважаючи на «роки індійсько-китайської дружби», носять, але оцінки обох країн, характер стратегічного суперництва).

8. Забезпечення підтримки сусідніми державами позицій КНР у суперечках із США та іншими країнами Заходу.

9. Фактичне утвердження «особливих відносин» між КНР та Монголією.

10. Придбання де-факто «особливого стану» у Центральній Азії.

11. Виключення шансів вступу інших країн до антикитайських коаліцій та військового протистояння з Китаєм.

12. Нав'язування іншим країнам торгово-інвестиційної політики, сприятливої для Китаю.

13. Визнання країнами регіону провідної регіональної ролі КНР, що виражається у вигляді неформальних, але обов'язкових консультацій із Пекіном перед прийняттям важливих зовнішньополітичних рішень.

14. Закріплення «особливих прав» китайських меншин за кордоном та визнання права Пекіна на їхній захист.

Отже, можна зробити висновок, що США та КНР – дві передові держави світу з власними цілями за завданнями, які мають неабиякий вплив на міжнародній арені. Науковці виділяють три зони безпосереднього зіткнення інтересів між КНР і США. Перша пов’язана з неминучим проникненням Пекіна на Близький Схід унаслідок стрибкоподібного зростання енергоспоживання економікою Китаю, що призведе до конфронтації зі США, Японією та іншими постіндустріальними державами, які вже облаштувалися в цьому регіоні. До цього прогнозу можна додати ще одну зону потенційних американо-китайських суперечностей із-за нафти і газу – Прикаспій і Центральна Азія. Наступну зону конфлікту, на переконання «оптимістів», формує політика багатополярності Пекіна, яка полягає у стимулюванні появи нових і посиленні старих центрів сили, що загалом нібито зменшує наддержавне значення американського центра. Третьою очевидною зоною зіткнення є Тайванська проблема.

РОЗДІЛ 2. СИСТЕМНИЙ ВИМІР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КНР ТА США

2.1 Стратегія інформаційної безпеки КНР на сучасному етапі

Китайський стратег і мислитель Сунь Цзи у своєму знаменитому трактаті «Мистецтво війни» висловив головну ідею китайської стратегії – воювати без зброї, перемагати без боя. Незважаючи на минулі літа і століття, мудрість не втратила актуальність. Провідні світові держави прагнуть вести протистояння із супротивником безкровними методами, а замість зброї дедалі частіше використовують інформаційні технології та ресурси. Але пальму першості в інформаційній війні впевнено зберігає Китай. Про це свідчать дані та звіти різних міжнародних та міжвідомчих комісій, що досліджують тенденції розвитку сучасних інформаційно-комунікаційних технологій (ІКТ) і виникають у зв'язку з цим загрози глобальній безпеці.

Під інформаційною безпекою в Китаї розуміється захист обладнання, програмного забезпечення, даних та послуг інформаційної системи, за винятком ймовірності несанкціонованого доступу до них, витоку, знищення або зміни з випадкових або зловмисних причин, перегляду, перевірки, запису або знищення з метою забезпечення безперервної та надійної роботи інформаційної системи.

Основними складовими інформаційної безпеки є справжність, конфіденційність, цілісність, безвідмовність, готовність і керованість. Національний інформаційний консультативний комітет КНР визначає інформаційну безпеку як ключовий компонент системи національної безпеки, який необхідний для забезпечення сталого, здорового застосування інформаційних технологій, а також для соціальної та культурної стабільності та ідеологічного розвитку.

Важливою складовою ІБ є безпека в інтернет-просторі на території Китаю та за його межами. Удосконалюються заходи щодо протидії інформаційно-технологічним загрозам, або кіберзагрозам (хакерство та хактивізм, виведення серверів з ладу, розкрадання та шпигунство, саботаж та руйнування, стратегічні атаки та

інформаційне протиборство), інформаційно-психологічному впливу, втручанню у внутрішні справи держави за допомогою інформаційно-комунікаційних технологій (ІКТ), терористичної та екстремістської діяльності у цій сфері. Крім того, швидко розвиваються такі новітні технології, як штучний інтелект, блокчейн, 5G зв'язок. Все більш серйозними стають проблеми у сфері великих даних, хмарних обчислень та інтернету речей. Серед них можна виділити високий ризик витоку даних, кібератаки та пов'язані з ними інтелектуальні злочини. Таким чином, з'являються нові загрози безпеці ключової державної інфраструктури КНР, приватного життя людей та соціальної стабільності.

Згідно з китайськими джерелами, витоки загроз інформаційній безпеці можна поділити на три складові:

1. Фактори ризику технічної безпеки: слабкий захист безпеки базової інформаційної мережі та важливих інформаційних систем та втрата конфіденційності. Перший фактор ризику пов'язаний з небезпеками для базової мережі Китаю, яка включає інтернет, телекомунікаційні, радіо- і телевізійні мережі. Критично важливою є державна інфраструктура: авіа- та залізничне сполучення, дороги, уряд, банки, цінні папери, електрика, цивільна авіація, нафта тощо. Хоча Китай і досяг певних результатів у захисті інформаційної безпеки в цих сферах, з його боку потрібні подальші серйозні дії.

Другий фактор ризику пов'язаний із загрозами конфіденційності, цілісності та доступності корпоративних та особистих даних на тлі збільшення їх сукупного обсягу та в умовах, коли втрати даних більше не піддаються виміру. З'являється все більше вразливостей, що ведуть до витоку даних через інтернет, і посилюється значення мобільного зв'язку, що означає нові цілі та завдання в галузі інформаційної безпеки.

2. Шкідливі атаки є найбільшою загрозою для інформаційної безпеки. Ретельно продумані атаки хакерів стали найбільш небезпечними для фізичних осіб і апаратних систем. Шкідливі атаки діляться на активні, метою яких є втручання у зміст інформації в системі та руйнування її достовірності та цілісності, та пасивні, націлені на перехоплення та розкрадання інформації без шкоди для використання мережі.

3. Слабке управління інформаційною безпекою, на думку деяких китайських експертів, є наслідком відставання досліджень у цій галузі КНР з інших розвинених країн. Інформаційна безпека Китаю досить тендітна ще й тому, що в минулому дослідженням в галузі ІБ приділялося мало уваги. У результаті комп'ютерна архітектура, зокрема комунікаційна, недостатньо захищена. У даний час перед КНР стоять завдання запровадження правил інформаційної безпеки та розробки стандартів оцінки ризиків систем управління інформаційною безпекою.

На основі законодавчої бази, офіційних урядових документів, таких як доктрини та стратегії, спеціальних програм розвитку, матеріалів з преси та промов голови Китайської Народної Республіки Сі Цзіньпіна розглядається еволюція політики Китаю в галузі інформаційної безпеки. Сфера кібербезпеки потрапила в поле зору китайської влади у другій половині 1990 років. Одним із стимулів розвитку законодавства в цій галузі послужило створення у 1999 році системи електронного державного управління (Government Online Project, GOP) та виникнення необхідності адекватного правового регулювання. Так, у 2000 році було прийнято керівні принципи для системи електронного державного управління (Guidelines of National Electronic Government Construction, NEGC).

У нормативно-правовому аспекті забезпечення інформаційної безпеки КНР слід зазначити такі документи, які є ключовими. У 2000 р. Всекитайськими зборами народних представників була спроба визначити класифікацію можливих правопорушень в інформаційній сфері. У тому ж році було опубліковано «Постанову ВСНП із захисту інтернет-простору», де виділялися ті галузі, в яких можуть здійснюватися порушення: економічна, освітня, сфера підтримки суспільної стабільності та захисту громадян. Виник прецедент, коли держава спробувала створити класифікацію ймовірних інформаційних загроз та згодом розробити заходи щодо забезпечення безпеки у цій сфері.

Проаналізувавши нормативно-правову базу було визначено базові документи щодо забезпечення внутрішньодержавної інформаційної безпеки КНР та структуровано в таблицю 2.1 у додатках.

1. Правила регулювання, забезпечуючи безпеку комп'ютерних та інформаційних систем (1994р.) – наділення Міністерства державної безпеки повноваженнями з контролю, інспекції та забезпечення національної ІБ, розслідування, розкриття та запобігання злочинам в області ІКТ.

2. План державної інформатизації в рамках 9-го п'ятиріччя та перспективні цілі до 2010 (1997р.) – позначення перспективних цілей ІБ, що передбачають інформатизацію всіх державних інфраструктур до 2010 р.

3. Закон про безпеку мережевої інфраструктури та мережі Інтернет (1997р.) – заборона використання мережі для створення, розповсюдження, копіювання або передачі певних видів інформації, до яких віднесені заклики до невиконання або порушення державних законів, терористичної діяльності або порушення цілісності країни.

4. Постанова Всекитайських зборів народних представників (ВСНП) про забезпечення безпеки в мережі Інтернеті (2000р.) – необхідність регулювання та моніторингу інформаційних відносин через значиму роль інтернету в економічному будівництві та інфраструктурі КНР.

5. Постанова державної інформатизованої керівної групи щодо роботі в галузі зміцнення інформаційної безпеки (2003р.) – необхідність зміцнення захисту критично важливої, стратегічної інфраструктури.

6. Державна стратегія розвитку інформатизації на період з 2006 по 2020 (2006р.) – план створення структур регулювання діяльності в інформаційній сфері, виробництво власного програмного забезпечення, визначення базових векторів державної політики у галузі ІБ.

7. Постанова Держради КНР щодо просування інформатизації та розвитку чинного захисту інформаційної безпеки (2012р.) – контроль над інтернет-додатками, віртуальними угодами у торговельно-економічній сфері, інформаційно-мовними послугами; затвердження осіб, які відповідають за заходи щодо забезпечення безпеки у регіонах; дозвіл застосування регіональною владою заходів щодо обмеження доступу до листування в інтернеті та інтернет-трафіку при виникненні загроз безпеці країни.

8. Антитерористичний закон КНР (2015р.) – дешифрування інтернет-трафіку, застосування адміністративних заходів щодо вилучення у іноземних компаній та підприємств інформації при підозрі у її використанні для терористичних цілей; запровадження цензури для діяльності новин на території КНР.

9. Закон КНР про кібербезпеку (2016р.) – необхідність вказувати реальні дані користувача при реєстрації, обов'язкове зберігання інформації, що публікується, протягом 6 місяців на території КНР.

10. Положення про захист безпеки критично важливої інфраструктури (2019р.) – захист критично важливої інформаційної інфраструктури від атак, вторгнень, втручання та знищення; просування державою безпечних та надійних мережевих продуктів та послуг; поліпшення стандартної системи мережевої безпеки.

11. Заходи з приводу оцінки безпеки хмар-них обчислень (2019р.) –введення відповідних заходів контролю при закупівлі та використанні продуктів, включених до каталогів спеціального мережевого обладнання безпеки; запровадження більш високих вимог безпеки для хмарних обчислень, які використовуються державними установами та операторами зв'язку.

12. Закон про шифрування даних (2020р.) – заборона порушення конфіденційності даних; необхідність вжити заходів у разі виникнення загроз інформаційній безпеці.

13. Закон КНР про безпеку даних (2021р.) – спрямовано регулювання відносин, що з обробкою даних. У новому економічному п'ятирічному плані наголошується на необхідності посилення впливу уряду на дані приватних компаній.

Проблематиці забезпечення національної безпеки в кіберпросторі КНР присвячені роботи американських дослідників Джона Ліндсей, Даніеля Вентре. У працях даних авторів зроблено спробу дати теоретичне обґрунтування функціонування державного апарату.

Китайська Народна Республіка в інформаційному просторі. Серед китайських досліджень необхідно виділити роботи Фан Бінь Сіна та Ван Гуйфана, які дотримуються офіційної позиції уряду Китайської Народної Республіки. Також китайські автори проводять порівняльний аналіз підходів до забезпечення

інформаційної безпеки КНР та США, спираючись на розгляд американської системи безпеки.

Останніми роками Китай звертає увагу на обробку даних. У новому економічному п'ятирічному плані наголошується на необхідності посилення впливу уряду на дані приватних компаній. Окрім названого Закону, обробка даних у Китаї також регулюється Законом про кібербезпеку 2017 року, що передбачає локалізацію даних на території КНР. Наразі закінчилися консультації щодо другого проекту Закону про захист персональних даних, яким регулюватимуться відносини, пов'язані безпосередньо з обробкою персональних даних. Очікується, що його буде прийнято до початку 2023 року. У перспективі ці три закони утворюють систему регулювання відносин, що з обробкою різних видів даних у КНР. Приймаються й інші нормативні акти регуляторів, які впливають на обробку даних у Китаї. Зокрема, 1 травня 2021 року набули чинності Положення про обсяг необхідних персональних даних для поширених типів мобільних додатків, якими обмежується обсяг оброблюваних персональних даних у різних типах мобільних додатків. Нормативні акти у цій сфері вже активно використовуються. Наприклад, китайський регулятор ухвалив заблокувати мобільний додаток компанії DiDi до приведення обробки персональних даних у відповідність до нових правил.

Регулювання сфери обробки даних Китаєм спрямовано насамперед встановлення переваги Китаю як цифрової держави на глобальній арені і недопущення створення альтернативних центрів сили як великих технологічних компаній у країні. Більше того, влада побоюється, що організації можуть ділитися даними з іноземними компаніями та державами, що підриває національну безпеку Китаю. Китай цим Законом наголошує, що дані, накопичені приватними компаніями, слід розглядати як національний актив, використання якого здійснюється або обмежується відповідно до потреб держави.

Сенс Закону полягає у створенні керованої державою системи захисту даних за допомогою встановлення державного контролю та доступу до даних. Цілями Закону вказуються стандартизація обробки даних, забезпечення безпеки даних, сприяння розробці та використанню даних, захист законних прав та інтересів фізичних осіб та

організацій КНР, а також захист національного суверенітету, безпеки та інших інтересів.

Закон встановлює, що держава має реалізувати стратегію щодо великих даних, у тому числі створити інфраструктуру даних, заохочувати та підтримувати інноваційне застосування даних у всіх галузях. У зв'язку з цим, держава повинна створити систему категоризації та класифікації захисту даних відповідно до міри важливості даних для розвитку держави (Multi-Level Protection System). Відповідно до такої системи накладаються різні вимоги безпеки залежно від збитків національної безпеки, громадських та інших інтересів, які можуть бути заподіяні при порушеннях безпеки даних. У тому числі це стосується зміни, знищення, витоку, незаконного отримання або використання даних у непередбачених цілях. На основі цієї системи також має бути створено «каталоги важливих даних».

Також держава створить механізм реагування на надзвичайні ситуації у сфері безпеки даних та механізм для перевірки безпеки даних. Крім того, мають бути створені каталоги відкритих державних даних. У Законі окремо зазначено, що при прийнятті дискримінаційних заборон та інших аналогічних заходів проти КНР іноземними державами Китай може вжити заходів у відповідь щодо таких держав. З метою національної безпеки та інших цілях може бути передбачений експортний контроль над передачею даних відповідно до законодавства КНР.

У Законі ключове місце займають терміни «національні ключові дані» (national core data) та «важливі дані» (important data). Національні ключові дані – дані, що впливають на національну безпеку, економіку та суспільні інтереси. Важливі дані як поняття не визначено у Законі чи інших нормативних актах. Оскільки важливі дані мають ключове значення для Закону, відсутність ухвали може створити правову невизначеність, як і у випадку із Законом про кібербезпеку 2017 року, щодо якого ще не було видано правил його застосування. Однак, як було зазначено вище, мають бути створені каталоги важливих даних, а також існують проекти підзаконних актів, у яких визначення важливих даних запроваджуються щодо конкретних сфер економіки. Наприклад, 12 травня 2021 року Управління кіберпростору Китаю (CAC) випустило

на громадське обговорення Проект Правил управління безпекою автомобільних даних, в якому викладено обсяг важливих даних для автомобільної промисловості.

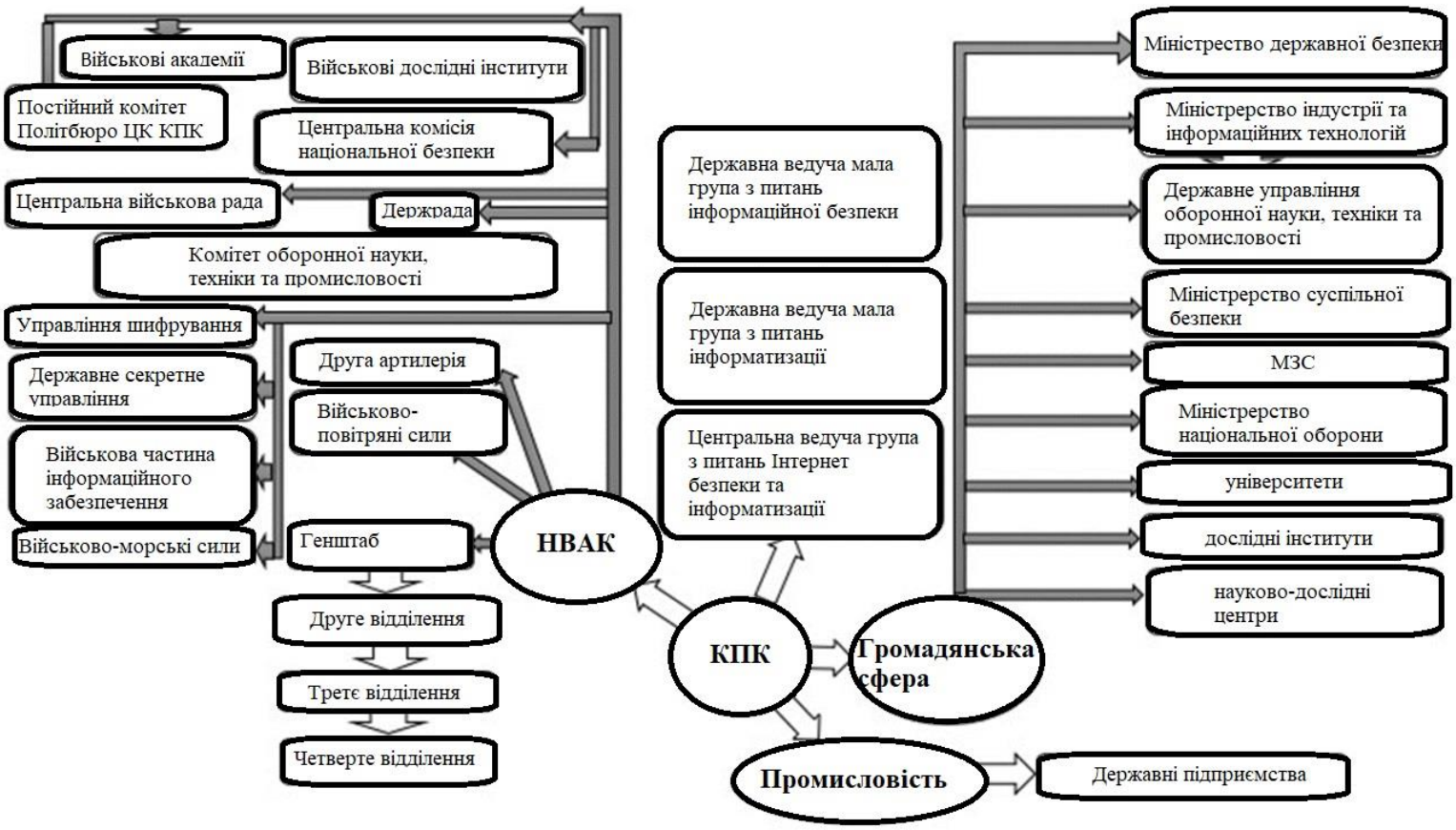

Рисунок 2.1 Структура державних органів КНР з реалізації політичних установок в інформаційному просторі [14].

1. Центральні органи КПК: Постійний комітет Політбюро; Центральна комісія з національної безпеки; Державна рада; цивільні урядові організації (міністерство промисловості та інформаційних технологій, міністерство державної безпеки, міністерство громадської безпеки).

2. Державне управління оборонної науки, техніки та промисловості.

3. Державне секретне управління.

4. Державне управління шифруванням.

5. Партійні та державні провідні групи та малі провідні групи.

6. Національний комітет безпеки.

7. Народно-визвольна армія Китаю (НВАК).

8. Підзвітні державі дослідні та наукові інститути.

9. Академічні інститути НВАК.

10. Науково-дослідні центри.

Рис. 2.2 Структура державного апарату КНР в області забезпечення інформаційної безпеки

Проаналізувавши інформаційний простір та політику КНР можна зробити два головних висновки:

1. Через фільтр «Золотий щит» КНР вдалося забезпечити значну ізоляцію інформаційного простору країни від зовнішнього проникнення небажаного контенту. Цей захід дозволив захистити суспільство КНР багатьох негативів Заходу (кольорові революції, тероризм та інших.) і цим забезпечити його монолітність за умов протидії численним загрозам із боку США. Проте державне замовлення на критерії селекції швидше відповідатиме запитам правлячої еліти, ніж потребам широких верств населення Китаю. Прорахунок у такому питанні загрожує стратегічними наслідками для розвитку нації, так як фільтрація контенту стосується всіх китайців одночасно і дії ці суто обмежувальні, які з точки зору психології особистості (тим більше в інформації) викликають внутрішній протест у людини, навіть якщо вона ставиться до такої покірної нації, яка проживає у Піднебесній. В цьому випадку «гігантський мурашник» перетворюється на киплячий котел без клапана з високими ризиками соціального вибуху. При цьому жорсткі інформаційні обмеження (особливо у користуванні настільки популярними зараз глобальними соціальними мережами)

відгороджує Китай від світової цивілізації, порушуючи повідомлення, такі необхідні для обміну досягненнями та зростання. Звинувачення в несанкціонованому запозиченні ідей та технологій щодо Китаю аж ніяк не безпідставні, але досягати вершин прогресу таким способом стає все важче, тому доведеться організовувати повноцінну дифузію контенту навіть із ризиком проникнення його деструктивних різновидів до інформаційного простору Китаю.

2. Глобальна цифровізація життєдіяльності громадян розвинутих країн природно відкриває мережевим адміністраторам найширші можливості контролю над своїми користувачами. Мультимережеве господарство сучасних мегаполісів дозволяє організувати чи не тотальне відстеження своїх мешканців на вулиці, роботі, в будинку, банку, торговельно-розважальних комплексах та інших об'єктах. Інтеграція таких мереж з технологіями великих даних дає можливість концентрувати та аналізувати відомості майже про кожну людину, що потрапила в поле зору вищезгаданої інформаційної павутини. Застосування засобів штучного інтелекту посилює тотальність спостереження. Яскравим прикладом тому може служити китайська система соціального кредиту, милозвучна назва якої фактично не приховує сутності функціоналу, що їй реалізується, що дозволяє налагодити цифрове стеження практично за кожним жителем КНР. Подібне обмеження свобод населення певною мірою виправдане для КНР.

Виклики, з якими доводиться стикатися до цієї держави, дуже масштабні. Жорстка геополітична конкуренція зі США за гігантського і досить різношерстого населення Піднебесної змушують уряд КНР вдаватися до радикальних засобів захисту свого суверенітету. Тому контроль над населенням буде тотальним, що, власне, забезпечує систему соціального кредиту.

Підходи КНР до мінімізації загроз у сфері ІБ.

Одним із основних підходів до мінімізації загроз ІБ у КНР є запобігання проникненню небажаної інформації всередину країни та витоку чутливої інформації за кордон, у т. ч. шляхом блокування соціальних мереж та пошукових систем. Керівництво КНР вважає, що саме поняття «інформаційна безпека» передбачає запровадження обмежень поширення небажаної інформації.

У Китаї існують різні погляди на вироблення загальносвітових стандартів інформаційної безпеки. Одним із основоположних підходів КНР є облік трьох сфер у забезпеченні ІБ: економічної, політичної та воєнної. У цьому наголошується на такі пріоритети:

1. Захист Комуністичної партії через інформаційний контроль та пропаганду, нагляд за внутрішніми джерелами потенційних заворушень.

2. Використання операцій комп'ютерної мережі, пов'язаних з оповіщенням про незадоволеність іноземних держав китайською політикою або приписуваними КНР діями за кордоном (такими, як морські територіальні суперечки або звинувачення Китаю в хакерській діяльності) негативно впливають на репутацію країни.

3. Підготовка до військових дій та забезпечення військової переваги у разі кіберконфлікту з противником у вигляді військової модернізації, дослідження операцій комп'ютерної мережі та розвитку людського капіталу.

4. Вивчення військової інфраструктури потенційних противників, їх мотивації, цілей, можливостей та обмежень в інформаційному просторі.

5. Просування альтернативних варіантів державного контролю та управління інформаційною безпекою на національному та міжнародному рівнях.

Уряд КНР сприймає інформаційну безпеку та інформатизацію як дві основні складові національної безпеки та національного розвитку Установа Китаєм «Комісії з національної безпеки», «Провідної Центральної групи» та «Провідної Малої групи з безпеки та інформатизації центральної мережі» була покликана визначити на найвищому рівні пріоритети ІБ та скоротити «цифровий розрив» між різними регіонами країни. На думку колишнього генерального секретаря КПК Сі Цзіньпіна, завдання використання інформаційних технологій для стимулювання індустріалізації, урбанізації, модернізації сільського господарства, національних систем управління та можливостей управління є однією з першорядних.

Політичне керівництво вважає актуальною проблемою забезпечення гарантій безпеки критично важливої інформаційної інфраструктури глобальної мережі. З іншого боку, найважливішою метою є подолання технологічної залежності Китаю від країн. Стратегія досягнення незалежності КНР у галузі ІКТ базується на

впровадженні власних технологічних інновацій та створенні конкуренції закордонним компаніям. Відповідно до наявних планів, до 2049 р. Китай планує зайняти лідируючу позицію у світі щодо впровадження інновацій. Досягнення цієї мети сприяють значні людські ресурси, що є у розпорядженні КНР: з більш ніж шести мільйонів щорічних випускників вузів близько 60–70% становлять науково-технічні фахівці та інженери.

2.2 Стратегія інформаційної безпеки США в умовах конфліктної взаємодії

Якщо виходити з реалій сьогодення, то слід визнати, що нині є лише одна наддержава – США, яка на офіційному рівні розглядає інформацію як певний стратегічний ресурс, який виникає в результаті обробки даних за допомогою спеціалізованих систем аналізу. Сполучені Штати одними з перших усвідомили стратегічну важливість безпеки кіберпростору. Слід зазначити, що США активно готуються і надалі до ведення інформаційної війни 21 століття. Більше того, у всіх збройних конфліктах, у яких брали участь США («Буря в пустелі», операція на Гаїті, агресія проти Югославії та ін.), було апробовано різні види інформаційної зброї.

Для того, щоб виявити стратегію інформаційної безпеки США в умовах конфліктної взаємодії, необхідно проаналізувати документи, законопроекти, ініціативи та державні стратегії, що вплинули на хід розвитку та становлення сучасної версії стратегії у просторі ІБ.

До перших офіційних документів Пентагону з проблеми ІБ можна віднести директиву МО США Т3600.1 від 21 грудня 1992 року під назвою «Інформаційна війна». У 1993 року у директиві Комітету начальників штабів № 30 було викладено основні засади ведення інформаційної війни. І, нарешті, 1997 року було дано таке визначення інформаційної війні: «Дії, вжиті задля досягнення інформаційного переваги у сфері національної стратегії і здійснювані шляхом впливу інформацію та інформаційні системи противника за одночасного захисту власної інформації та своїх інформаційних систем».

Перші основи американської військової стратегії ІБ було закладено 1990-ті роки. У період адміністрації Білла Клінтона в 1995 році була оприлюднена Стратегія національної безпеки, де було поставлено завдання: шляхом наступальних та оборонних інформаційних операцій досягти інформаційної переваги.

У червні 1995 року Національний університет оборони у Вашингтоні здійснив випуск першої групи спеціалістів у галузі інформаційної війни. Місяцем пізніше у Військово-морському коледжі в Ньюпорті було завершено ігрове відпрацювання планів ведення інформаційних воєн. У січні – червні 1995 року в США було проведено командно-штабну військову гру (КШВІ), за участю представників усіх силових структур. Її ціль – розробка концепції стратегічної інформаційної війни.

Директива Президента № 63 «Про захист критичної інфраструктури», підписана президентом США у 1998 році, отримала розвиток та була кодифікована у вигляді «Національної стратегії безпеки кіберпростору». Також вона була кодифікована у вигляді Директиви Президента в галузі національної безпеки №7 «Про визначення, пріоритизацію та захист критично важливих елементів інфраструктури», причому в обох документах особливий пріоритет мало створення програми з мінімізації загроз у кіберпросторі.

Незабаром після терористичних атак 11 вересня 2001 року, які виявили вразливість національної безпеки, адміністрація Джорджа Буша інтенсифікувала роботу щодо розвитку конкретних механізмів забезпечення ІБ. Так, у 2003 році була розроблена Національна стратегія із забезпечення безпеки кіберпростору, в якій адміністрація Буша визначила основні програми, спрямовані на забезпечення національної кібербезпеки, запобігання кібератакам та зменшення вразливості критичної інфраструктури. У стратегії також наголошувалося на значущості досягнення переваги завдяки наступальним і оборонним інформаційним операціям. Міністерство оборони виділило три випадки їх застосування: у мирний час, у період кризи і під час конфлікту, що показує вже тоді наміри керівництва країни посилити свої сили в кіберсередовищі, щоб бути готовими і до інформаційної оборони.

Стратегія 2003 року отримала своє продовження вже у 2008 році, коли було прийнято Комплексну ініціативу з національної кібербезпеки. Цією ініціативою було

закладено основу для подальшої розробки ІБ країни, вона підтвердила, що в майбутньому кіберзагрози вимагатимуть ще більших зусиль від уряду щодо впровадження своїх технічних, а також організаційних можливостей для більш дієвих рішень сучасних загроз та вразливостей.

У грудні 2006 року КНШ підготував документ «Національна військова стратегія кібернетичних операцій» (наразі частково розсекречений), який серед іншого визначив стратегічні пріоритети проведення операцій із забезпечення інформаційної безпеки США:

1. Досягнення та утримання ініціативи в ході операцій, що проводяться всередині циклу прийняття рішення противником.

2. Забезпечення захисту власних комп'ютерних систем та здійснення наступальних дій у комп'ютерних мережах противника.

3. Включення операцій у кіберпросторі до системи військового планування для всього спектра збройних конфліктів з метою вироблення методів ведення таких операцій (з урахуванням особливостей різних ТВД) у тісній взаємодії з видами ЗС та управліннями МО, які, у свою чергу, мають узгоджувати свої дії з іншими відомствами США, союзниками з коаліції та промисловими підрядниками.

4. Створення в рамках міністерства оборони необхідних умов для проведення кібернетичних операцій, включаючи організаційні заходи, підготовку спеціалістів та створення відповідної інфраструктури.

5. Оцінка ризиків мережевих операцій, які можуть виникнути через недостатньо ефективний підбір коштів або зустрічного використання противником уразливих місць у кіберпросторі США, а також внаслідок побічного ефекту від проведення наступальних операцій.

За даними Пентагону, лише у 2007 році зареєстровано майже 44 тис. інцидентів, які були кваліфіковані як кібернетичні злочини, вчинені іноземними арміями, спецслужбами та окремими хакерами. Одним з найбільших випадків такого роду стало розкрадання декількох терабайт даних про багатоцільового винищувача-бомбардувальника п'ятого покоління F-35 «Лайтнінг-2», що розробляється в США.

Вартість проекту бойового літака становить близько 300 млрд. доларів. Передбачається, що дані викрали з серверів компаній-підрядників.

Необхідно відзначити, що незважаючи на те, що ІБ США почала розвиватися ще в 90-ті роки і продовжила свій розвиток у 2000-ті, саме з приходом адміністрації Барака Обами розпочався принципово новий етап розвитку у напрямку даного простору. Президент Обама спочатку визначив ІБ як одну з найсерйозніших проблем у безпеці країни, що при цьому зачіпає економічну сферу. Незабаром після вступу Барака Обами на посаду їм було доручено провести розгляд федеральних заходів із захисту американської інформаційної інфраструктури.

У травні 2011 року Білий дім представив світові Міжнародну стратегію в кіберпросторі, в якій було наголошено на необхідності військового стримування та протистояння, створення мирного та стабільного глобального кіберпростору завдяки міждержавному співробітництву. У документі виділялося визнання та пристосування зростаючої військової потреби у надійних та безпечних мережах. Крім того, американці визнали важливість і необхідність розширення існуючих військових союзів для протистояння потенційним загрозам у кіберпросторі. Представлена Міжнародна стратегія показала відкритість американської адміністрації до співпраці з іншими країнами, а також вкотре наголосила на яких принципах вони самі дотримуються.

Пізніше, у липні 2011 року, також у період адміністрації Обами, було прийнято Стратегію дій Міністерства оборони у Кіберпросторі, що було першим документом, що визначає політику Міністерства оборони у кіберпросторі. Опір був на безпеку та надійність нового простору ІБ, який повинен захищати основні свободи всіх громадян, недоторканність їхнього приватного життя, а також повністю вільні потоки інформації, які необхідні для своєчасного зв'язку при здійсненні військових місій.

Однією з головних проблем ІБ, що хвилювали США, залишалось комерційне шпигунство з боку Китаю, однак укази, що видавались, не сприяли поліпшенню ситуації. І наступним важливим кроком у її розвитку стало прийняття у 2012 році Національної Стратегії обміну та захисту інформації. Цей документ визначив три основні принципи політики США щодо інформаційної безпеки: інформація як

національне надбання; обмін та захист інформації, що вимагало поділу загальних ризиків; прийняття кращих рішень завдяки інформації. Пояснити прийняття нової стратегії можна тим, що американський кіберпростір продовжував зазнавати безлічі атак, адміністрація намагалася знайти нові, іноді навіть інноваційні способи захисту інформаційних мереж та структур.

Підсумком усіх попередніх стратегій можна назвати оприлюднену в ніч на 24 квітня 2015 року Міністерством оборони США оновлену стратегію ІБ країни, в якій знову було встановлено прагнення стримувати будь-які кібератаки і максимально захищати Сполучені Штати від будь-якого супротивника та інформативного вторгнення. У стратегії були присутні і вперше виділені потенційні вороги в кіберпросторі, визначивши три групи загроз: окремі держави (Китай, Росія, Іран та Північна Корея); недержавні актори (Ісламська держава); кіберзлочинці.

19 грудня 2017 року адміністрацією Дональда Трампа було опубліковано документ «Стратегія національної безпеки США», де Китай представлений одним із суперників США, але вже зазначено, що він прагне змінити глобальне розміщення сил у власних інтересах, а це може спричинити загрозу Сполученим Штатам. МЗС Китаю негайно відреагувало і у відповідь на це звинувачення заявило, що Вашингтону слід відмовитися від застарілих концепцій.

19 січня 2018 року міністерство оборони США оприлюднило нову Стратегію національної оборони США (National Defense Strategy). У цьому документі було заявлено, що головною проблемою національної безпеки США надалі розглядатиметься не тероризм, а стратегічне суперництво між державами. п'ятьма головними загрозами американської безпеки в документі було названо чотири держави (Китай, Росія, КНДР, Іран) і активність терористичних угруповань, що продовжується.

У березні 2021 року президент Джо Байден опублікував Тимчасову стратегію національної безпеки (NSS) на 2021 рік, яка знову прив’язала Сполучені Штати до альянсу НАТО та окреслила глобальні пріоритети країни, зробивши висновок, що Сполучені Штати «повинні продемонструвати, що демократії все ще можуть приносити користь для нашого народу».

Включення функцій щодо забезпечення інформаційної безпеки до складу функцій Міністерства національної безпеки та інших аналогічних установ пояснюється тим, що атаки на інформаційну інфраструктуру потенційно можуть спричинити негативні наслідки для різних життєво важливих галузей економіки США: фінансового сектора, енергетики, транспорту та інших.

Крім того, в рамках окремих федеральних міністерств та відомств було створено спеціальні підрозділи, що вирішують окремі завдання у рамках загальної стратегії забезпечення інформаційної безпеки США:

1. Група готовності до надзвичайних ситуацій в інформаційних системах – United States Computer Emergency Readiness Team, US-CERT (підрозділ, що функціонує у складі DHS).

2. Армійський центр безпеки та підтримки роботи глобальних мереж – Army Global Network Operations and Security Center, AGNOSC (підрозділ, що функціонує у складі Міністерства оборони США).

3. Агентство оборонних інформаційних систем Міністерства оборони США (DISA), під управлінням якого знаходиться Об'єднаний центр забезпечення роботи комп'ютерних мереж – Joint Task Force for Computer Network Operations, JTF-CNO.

4. Центральна служба безпеки (Central Security Service, CSS) Агентства національної безпеки, National Security Agency – NSA.

Таким чином, загальна організаційна структура державного управління у сфері інформаційної безпеки в США є досить складною і складається з множини щодо самостійних і при цьому взаємопов'язаних елементів, основні з яких представлені на рис. 2.3.

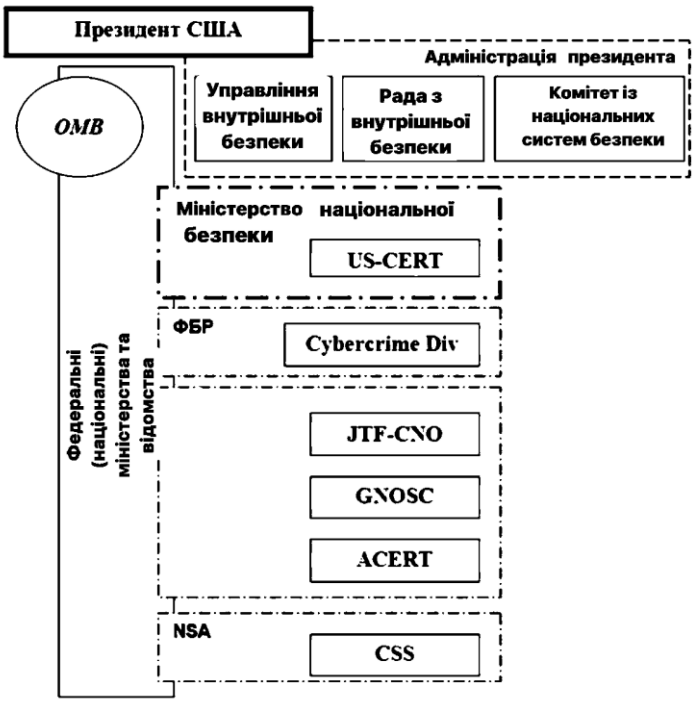

Рис. 2.3 Структура органів управління виконавчої влади, які вирішують завдання щодо забезпечення інформаційної безпеки США [36].

Комітет з національних систем безпеки (Committee on National Security Systems, CNSS) складається з 21 члена та 11 спостерігачів з числа фахівців різних федеральних відомств. Робота Комітету ведеться у межах кількох робочих груп. Цей комітет формує централізовану державну політику щодо окремих технологій та методів, важливих для захисту інформаційної інфраструктури на загальнонаціональному рівні. Зокрема, робота ведеться за такими напрямками, як:

1. Управління ризиками.

2. Засоби ідентифікації користувачів та пристроїв.

3. Стійкість мережної інфраструктури.

4. Розвиток системи підготовки кадрів у сфері інформаційної безпеки.

5. Забезпечення надійності у разі розширення спільного доступу до інформаційних ресурсів.

Основними інструментами досягнення цілей у цих напрямках є:

1. Розвиток національної політики у сфері інформаційної безпеки, а також розробка стандартів.

2. Оцінка рівня розвиненості існуючих та використовуваних засобів захисту інформації.

3. Випуск директив, інструкцій та технічних бюлетенів з певних проблем інформаційної безпеки.

4. Заснування нових урядових структур на вирішення спеціалізованих завдань.

5. Участь у регулюванні експорту засобів захисту інформації.

Міністерство національної безпеки (Department of Homeland Security, DHS), створене у листопаді 2002 року в процесі найбільшої реорганізації державного апарату як самостійний постійно діючий орган федеральної влади, поряд з вирішенням різних завдань, пов'язаних з безпекою США (таких як протидія тероризму та зовнішнім загрозам, а також запобігання наслідкам стихійного лиха), покликане виконувати такі основні функції у сфері інформаційної безпеки:

1. Розробка та вдосконалення загальнонаціонального плану щодо забезпечення безпеки ключових ресурсів та елементів інфраструктури Сполучених Штатів.

2. Здійснення управління кризовими ситуаціями під час атак на найважливіші інформаційні системи.

3. Надання технічної підтримки приватним компаніям та різним урядовим організаціям для усунення наслідків збоїв у разі порушення роботи критично важливих інформаційних систем.

4. Координація дій з федеральними структурами з метою своєчасного оповіщення різних підприємств та організацій про виникаючі загрози та заходи, які необхідно вжити.

5. Виконання, і навіть фінансування науково-дослідних робіт, необхідні вирішення завдань внутрішньої безпеки.

Функції забезпечення інформаційної безпеки належать Управлінню кібер-безпеки та комунікацій (Office of Cyber Security and Communications). У складі цього управління функціонує підрозділ, безпосередньою функцією якого є вирішення проблем, пов'язаних з інформаційною безпекою – National Cyber Security Division, до якого, у свою чергу, включений USCERT.

Група готовності до надзвичайних ситуацій в інформаційних системах (United States Computer Emergency Readiness Team, US-CERT) є центральним цілодобово функціонуючим органом, який відповідає за взаємодію з урядовими структурами (як федеральними, так і місцевими), а також іншими суб'єктами з питань захисту інформації. Її основним обов'язком є збирання та поширення інформації з метою реагування на інциденти, підвищення рівня скоординованості дій, зниження рівня вразливості. Група включає п'ять підрозділів.

1. Відділ поточної діяльності (Operations Branch). Відповідає за обробку одержуваної інформації про інциденти, забезпечує реагування на інциденти, розповсюджує необхідну інформацію, а також забезпечує аналіз різних даних з метою підвищення якості оцінки відомих або нових загроз для критично важливих елементів національної інфраструктури (включно з аналізом мережної інфраструктури, аналізом шкідливого ПЗ та ін.).

2. Відділ ситуаційної поінформованості (Situational Awareness branch). Відповідає за комплексний аналіз мережевої активності (тенденцій та характеру змін завантаження магістральних мереж) та інформування федеральних структур з метою підвищення рівня їхньої захищеності. Також забезпечує підтримку у вирішенні інцидентів.

3. Слідчий відділ (Law Enforcement and Intelligence branch). Забезпечує взаємодію з правоохоронними органами при виявленні та розслідуванні протизаконних дій.

4. Відділ перспективного розвитку (Future Operation Branch). Відповідає за розробку перспективних планів, процедур, регламентів, які забезпечують роботу US-CERT щодо реагування на інциденти.

5. Відділ підтримки (Mission Support branch). Забезпечує підтримку засобів комунікації, необхідних для роботи USCERT, включаючи підтримку веб-сайту, а також відповідає за адміністративну підтримку, безпеку персоналу, постачання та інші допоміжні функції.

Агентство оборонних інформаційних систем (Defense Information Systems Agency, DISA) Міністерства оборони США виконує безліч функцій, пов'язаних із

підтримкою військових інформаційних систем, і, зокрема, функції, пов'язані із забезпеченням їх надійності та безпеки.

До складу сил, відповідальних за інформаційну безпеку армії США, також входять:

1. Перше командування інформаційними операціями американської армії (U.S. Army's 1st Information Operations Command (LAND) (1ST IOC[L])), раніше відоме як Підрозділ з наземних військових інформаційних операцій (Land Information Warfare Activity, LIWA).

2. Морське командування оборонними операціями у кіберпросторі (Navy Cyber Defense Operations Command).

3. Армійський центр реагування на небезпеку інформаційної безпеки (ACERT).

Крім перерахованих функцій органів федеральної влади, державна політика інформаційної безпеки також наказує іншим установам сприяти вирішенню проблем інформаційної безпеки:

1. Національному науковому фонду – надавати фінансову підтримку науковим дослідженням у сфері інформаційної безпеки.

2. Державному департаменту – надавати різним органам необхідну допомогу при здійсненні міжнародного співробітництва у сфері інформаційної безпеки.

3. Центральному розвідувальному управлінню – протистояти проникненням до інформаційних систем з-за кордону.

4. Національний інститут стандартів (NIST), в особі Управління з комп'ютерної безпеки, що складається з чотирьох груп, – розробляти необхідні стандарти у сфері інформаційної безпеки.

5. Міністерству оборони – надавати технічну допомогу при розробці та впровадженні систем захисту інформації.

6. Міністерству юстиції та Федеральному бюро розслідувань – забезпечувати ефективне розслідування та припинення кіберзлочинів, а також здійснювати юридичну підтримку органів федеральної влади при вирішенні різноманітних питань, пов'язаних з інформаційною безпекою.

У складі законодавчої гілки влади – Конгресу США – основним структурним підрозділом, який відповідає за вирішення проблем інформаційної безпеки, є один із 22 постійних комітетів Палати представників – Особливий комітет національної безпеки (Select Committee on Homeland Security). Основним профільним підкомітетом є Підкомітет з нових загроз, кібербезпеки та науки (Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology). До сфери його інтересів входять питання, пов'язані з безпекою комп'ютерних систем, телекомунікацій, інформаційних технологій, систем автоматичного управління в промисловості, а також питання запобігання внутрішнім та зовнішнім атакам на урядові та приватні мережі, збитків, завданих цивільному населенню внаслідок атак на інформаційні системи.

Деякі слухання з питань інформаційної безпеки також може проводити Комітет з енергетики та торгівлі (Committee on Energy and Commerce). Зокрема, цими проблемами може займатися Підкомітет з питань телекомунікацій та мережі Інтернет (Subcommittee on Communications, Technologies, and the Internet).

До складу завдань Конгресу у сфері управління інформаційною безпекою, як і у всіх інших сферах державного управління, відповідно до Конституції країни входять:

1. Ухвалення законодавства.
2. Прийняття бюджету та управління фінансами.
3. Контроль за діяльністю урядових установ.
4. Виконання квазісудових функцій.
5. Формування структури виконавчої та судової влади.

Однією з основних форм роботи Конгресу та, зокрема, Комітету з національної безпеки та Комітету з енергетики та торгівлі, є проведення спеціальних слухань та розслідувань. Слухання проводяться з метою визначення напрямів удосконалення законодавства, виявлення та припинення недоробок та порушень у роботі органів виконавчої гілки влади тощо. Конгрес може розглядати як питання, пов'язані з національною безпекою та інформаційною безпекою державних структур, так і проблеми інформаційної безпеки приватного сектору та громадян країни. Для участі у слуханнях з різних питань, пов'язаних з інформаційною безпекою, до Конгресу, як

правило, запрошуються керівники та експерти, які представляють різні сфери діяльності:

1. Представники урядових установ, до чиєї компетенції входить забезпечення інформаційної безпеки (таких як NSA та ін.).

2. Керівники великих приватних компаній, що є лідерами у виробництві інформаційних систем та наданні інформаційних послуг (таких як Microsoft, ISS та інших).

3. Аредставники авторитетних науково-дослідних установ, консалтингових компаній, професійних та галузевих об'єднань (таких, як Electronic Industries Alliance).

Крім організації роботи окремих відомств, одним із важливих напрямів діяльності держави є підтримка програм спільної діяльності у сфері інформаційної безпеки всіх державних установ, а також приватних компаній.

Однією з основних таких ініціатив є Міжрегіональний Центр обміну та аналізу інформації, що об'єднує структури, що відповідають за інформаційну безпеку, в урядах практично всіх штатів. Завдання цього об'єднання:

1. Обмін інформацією про інциденти.

2. Поширення практично випробуваних методів та прийомів забезпечення безпеки.

3. Поширення попереджень про нові загрози інформаційній безпеці.

Крім того, однією з федеральних ініціатив є Національне партнерство з підвищення надійності інформації – National Information Assurance Partnership, NIAP, створене для підтримки розробки надійних IT-продуктів та перевірки інформаційних систем на відповідність міжнародним стандартам у сфері інформаційної безпеки. Завдання цієї структури:

1. Оптимізація витрат урядових та приватних структур на оцінку інформаційних систем.

2. Заохочення створення приватних структур, які займаються перевіркою безпеки інформаційних продуктів.

3. Підвищення доступності інформаційних систем, що пройшли належну перевірку на відповідність сучасним стандартам.

Також до загальнофедеральних програм належить Інформаційна мережа для попереджень про загрози критичної інфраструктури (Critical infrastructure Warning Information Network, CWIN), основним завданням якої є надання можливості обміну попередженнями та передачі сигналів тривоги між урядовими організаціями, а також приватними компаніями та деякими зарубіжними партнерами. За задумом Міністерства національної безпеки, дана мережа має забезпечити надійний зв'язок з різними суб'єктами, чия участь є принципово необхідною для відновлення критично важливої інфраструктури у разі подій національного масштабу.

Американська адміністрація вважає, що формування єдиної глобальної інформаційної інфраструктури під контролем США дозволить їм вирішити завдання стратегічного використання інформаційної зброї «аж до блокування телекомунікаційних мереж держав, які не визнають реалії сучасної міжнародної системи».

Слід зазначити, що у час застосування інформаційних технологій у військових цілях мало регулюється міжнародним правом. На думку зарубіжних експертів, ці питання мають розглядатися та вирішуватися на багатосторонній основі за участю всіх зацікавлених сторін. При цьому управління інформаційним простором необхідне для забезпечення не тільки національної безпеки абсолютного IT-лідера США, але й міжнародної безпеки в цілому. Проте з цих питань США займають особливу позицію і уникають домовленостей.

РОЗДІЛ 3. ПРОБЛЕМИ ТА ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВ В УМОВАХ ГЛОБАЛЬНОГО ПРОТИСТОЯННЯ

3.1 Інформаційна безпека держави в контексті регулювання Тайванської проблеми

Ключовим пунктом протиріч у відносинах Китаю та США залишається напружена атмосфера навколо острова Тайвань. З точки зору КНР присутність збройних сил Сполучених Штатів на острові є головною перешкодою для досягнення стратегічних цілей Китаю, а саме: возз'єднання Китаю. КНР розглядає острів як 23-у провінцію країни і заявляє про свої історичні права на територію. США, виконуючи свої союзницькі зобов'язання і зберігаючи баланс сил у регіоні, що встановився після громадянської війни в Китаї, з китайської точки зору, втручаються у внутрішні справи КНР. США підтримують альтернативну модель капіталістичного Китаю без комуністичної надбудови, до якої Китай, ймовірно, і повинен прийти в ході подальшого розвитку країни, чого не може допустити існуючий режим.

Так, Г. Кісінджер вважав, що тайванське питання може бути одним з потенційних каталізаторів регіонального конфлікту між Сполученими Штатами та Китаєм. «Таке справді може статися, якщо обидві сторони відкинуть у бік стриманість, що характеризує взаємовідносини США та Китаю з цього питання вже не один десяток років. Однак таке розвиток подій далеко не неминуче. Майже всі країни визнають позицію Китаю, що полягає в тому, що Тайвань – невід'ємна частина країни. Так само вчинили вже сім президентів Сполучених Штатів, причому представляли обидві партії».

Позиція США. Сьогодні все більшу настороженість Китаю викликає відхід Сполучених Штатів від політики «єдиного Китаю», якої дотримуються більшість партнерів країни, як у регіоні, так і в Європі та Південній Азії. Принцип «єдиного Китаю» має на увазі визнання Тибету невід'ємною частиною КНР та політичну єдність країни, включаючи територію острова Тайвань. США ж прагнуть не лише підірвати цю політику, всебічно підтримуючи глобальну боротьбу за незалежність

Тибету, а також вибудовуючи незалежні відносини з Тайванем, продаючи зброю, створюючи систему протиракетної оборони.

Необхідно зазначити, що у питанні Тайваню Сполучені Штати керуються, насамперед, актом про відносини до Республіки Китай від 1979 року, шістьма поправками до акту 1982 року і трьома комюніке. У цих документах США висловлювали наміри мінімізувати неофіційні відносини з Республікою Китай. Загалом Штати визнавали політику «єдиного Китаю», у межах якої неможливо розглядати Тайвань як незалежну територію, проте вони історично не давали оцінки цієї політики. Відношення це змінювалося від адміністрації одного президента до наступної адміністрації.

США також необхідно враховувати позицію самого Тайваню, де громадська думка різноспрямована: одні виступають за збереження статус-кво; інші вимагають якнайшвидшої незалежності Тайваню (як, наприклад, колишній президент КР, громадський та політичний діяч Лі Денхуей), оскільки впевнені у гарантіях безпеки з боку США. Побоюючись потенційного загострення ситуації та можливої відмови США у підтримці Тайваню, КР підтримує свої збройні сили на хорошому рівні.

У лютому 1972 р. під час інтенсивних переговорів під час візиту Ніксона Вашингтон і Пекін виступили із спільною заявою в Шанхаї – першою з трьох комюніке, які протягом десятиліть служили опорою для політики США, що зачіпає Тайвань і Китай. У цьому першому комюніке, глибокому компромісі між Вашингтоном і Пекіном зазначалося, що «Сполучені Штати визнають, що всі китайці з обох боків Тайванської протоки вважають, що існує лише один Китай і що Тайвань є частиною Китаю. Уряд Сполучених Штатів не заперечує цієї позиції».

У другому комюніке 1979 р. адміністрація Картера встановила дипломатичні відносини з Пекіном і визнала «позицію Китаю, згідно з якою існує лише один Китай, а Тайвань є частиною Китаю», визнала КНР «єдиним законним урядом Китаю» та заявила, що «народ Сполучених Штатів будуть підтримувати культурні, торговельні та інші неофіційні відносини із народом Тайваню». Коротше кажучи, Вашингтон розірвав офіційні стосунки з Тайбеєм, щоб налагодити стосунки з Пекіном.

Конгрес прийняв суворий Закон про взаємини з Тайванем 1979 року (TRA). TRA, серед іншого, заявляє, що політика США полягає в тому, щоб: «розглядати будь-які спроби визначити майбутнє Тайваню іншими засобами, окрім мирних, у тому числі шляхом бойкотів чи ембарго, як загрозу миру та безпеці в регіоні Західної частини Тихого океану та інших країнах» викликає серйозне занепокоєння для Сполучених Штатів»; «підтримувати здатність Сполучених Штатів протистояти будь-якому застосуванню сили або іншим формам примусу, які можуть поставити під загрозу безпеку чи соціальну чи економічну систему народу Тайваню»;

США також створили Американський інститут на Тайвані (AIT) як квазі-посольство, засноване Конгресом. 17 серпня 1982 року Сполучені Штати, тоді очолювані президентом Рональдом Рейганом, і Китай опублікували остаточний варіант Трьох комюніке. У цьому документі зазначено позицію КНР про те, що «питання про Тайвань – це внутрішня справа Китаю»; заявлено, що Вашингтон «не має наміру зазіхати на суверенітет і територіальну цілісність Китаю, або втручатися у внутрішні справи Китаю, або проводити політику «двох Китаїв» або «одного Китаю, одного Тайваню»; і також заявлено, що Сполучені Штати прагнутимуть «поступово скорочувати продаж зброї Тайваню, що призведе з часом до остаточної резолюції».

Відносини між двома сторонами протоки знову стали нестабільними, коли Пекін ухвалив Закон 2005 року, який дозволив КНР використати «немирні засоби» для запобігання незалежності Тайваню за певних обставин. У тому ж році Буш сказав в інтерв'ю, що «якщо Китай вторгнеться в односторонньому порядку, ми відреагуємо на кшталт Закону про відносини з Тайванем. Якщо Тайвань оголосить незалежність у односторонньому порядку, це буде одностороннє рішення».

У листопаді 2020 року контр-адмірал США Майкл Студеман без попередження прибув на острів. А 9 січня 2021 року колишній держсекретар Помпео зняв усі обмеження, що регулюють взаємодію між США та урядом Тайваню. Колишній президент Трамп також підписав Закон про повноваження національної оборони на 2017 фінансовий рік, який спонукав міністра оборони «проводити програму обміну старшими офіцери». Було прийнято закон про поїздки на Тайвань 2018 року, в якому йдеться, що уряд США має сприяти «візитам між офіційними особами зі Сполучених

Штатів та Тайваню на всіх рівнях», та Закон про гарантії Тайваню 2020 року, який закликає до регулярних продажів зброї Тайваню.

Уряд держави-острова спільно з Американським інститутом на Тайвані (AIT), що представляє інтереси США, в 2020 році анонсували проведення кібернавчань. Для Тайваню, за словами Вірла Ноувенса (Veerle Nouwens) з Британського Королівського інституту досліджень у галузі оборони та безпеки UK, материковий Китай розглядається як одне з основних джерел кібератак на острові. Гендиректор Тайванського агентства кібербезпеки, також зазначає Ноувенс, повідомив про близько 30 мільйонів кібератак на місяць на урядові мережі, і близько половини цих нападів походить з КНР. Кібернаступальні та захисні навчання були офіційно запущені в.о. директора AIT Реймондом Гріном (Raymond Greene) на організованому Microsoft заході. Він охарактеризував їх як «позначення нового кордону» у кіберспівпраці Вашингтона та Тайбею.

Адміністрація Байдена у своїй заяві від 23 січня 2021 року, підкреслила симпатію до Тайваню, підтвердивши «давні зобов'язання» Сполучених Штатів: «Як зазначено у трьох комюніке, Законі про відносини з Тайванем і шістьма гарантіями». Він також пообіцяв «продовжувати допомагати Тайваню у підтримці достатнього потенціалу самооборони», підкреслюючи при цьому, що «наша прихильність до Тайваню непохитна».

Отже, історія взаємин між Китайською Народною Республікою (КНР) та Китайською Республікою (а саме так перекладається сама назва невизнаної держави на території о. Тайвань), яку сам Пекін по праву вважає своєю провінцією, у багатьох аспектах є унікальним явищем, коріння якого сягає історичних процесів минулого сторіччя.

Позиція КНР. Влада КНР вважає Тайвань невід'ємною частиною Китаю і вказує, що до Громадянської війни острів входив до складу країни де-юре та де-факто. Проте у 1940-х США підтримали партію Гоміньдан, прихильники якої згодом переселилися на Тайвань. З того часу Захід, за версією Китаю, підтримує напруженість у регіоні та не дає двом частинам одного цілого возз'єднатися.

Наприкінці 1970-х Пекін встановив дипломатичні відносини зі США (які заради цього розірвали офіційні відносини з Тайванем, хоча і продовжували надавати йому економічну та військову допомогу). У 1992 китайське керівництво, налагодивши відносини зі США і що стало на шлях ринкових реформ, розпочало з Тайванем переговори про мирне возз'єднання. Але 11 липня 1999 вони були перервані після того, як тайванський президент Лі Денхуей оголосив, що КНР і Тайвань – це «дві країни по обидва боки Тайванської протоки». Щодо позиції КНР, то з часом вона стає більш рішучою. У лютому 2000 року уряд КНР опублікував другу Білу книгу з тайванського питання, яка мала назву «Принцип одного Китаю та тайванське питання». У ній КНР вперше офіційно додала нову, третю за рахунком, умову застосування військової сили проти острова – «якщо тайванське уряд протягом тривалої години відмовлятиметься від мирного вирішення об'єднання сторін Тайванської протоки шляхом переговорів». Фактично це означало істотне посилення позиції Пекіна, який раніше говорив лише про дві умови, – «якщо Тайвань відокремиться від Китаю під будь-яким назвою і якщо Тайвань буде завойований та окупований іноземною державою». Третя умова давала набагато більше приводів для застосування сили Пекіном, а також її надмірне визначення дозволяло КНР удало використовувати цю умову на свою користь.

14 березня 2005 року Всекитайські збори народних представників (ВСНП) схвалили закон «Про протидію розколу країни». Цей документ передбачає право уряду КНР застосувати «немирні або інші необхідні заходи для захисту свого суверенітету та територіальної цілісності» у разі спроби «підривних елементів, що виступають за незалежність Тайваню», відокремити острів «від Батьківщини», або у разі «важливих змін, які можуть призвести до відокремлення Тайваню від країни, або якщо всі умови для мирного об'єднання будуть вичерпані». Прийнятий документ, який законодавчо закріплює можливість застосування сили, щоб запобігти проголошенню островом незалежності, розцінюється спостерігачами як спроба посилити психологічний тиск на Тайвань та схилити його до переговорів про мирне возз'єднання на умовах Пекіна.

У 2008 році президентом Тайваню був обраний Ма Іньцзю, представник партії Гоміндан, що дотримуються більш лояльних позицій. Незважаючи на відчутне пом'якшення міжберегових суперечностей у часи адміністрації Ма Інцзю і зниження ймовірності того, що тайванське питання стане причиною конфлікту між Китаєм і Америкою, історичні розбіжності між Пекіном і Вашингтоном щодо Тайваню так і не були вирішені. Перемога на тайванських президентських виборах кандидата ДПП Цай Інвен стала новим викликом для відносин між КНР і США. Свою лепту в загострення ситуації, як завжди, роблять США, для яких розпалювання регіональних конфліктів – цілком звична справа. Заради власного домінування на світовій політичній арені Вашингтон продовжує прибігати до будь-яких методів. І пропозиція постачання озброєння Тайваню – якраз із цієї серії. Зрозуміло, що така пропозиція здатна перекреслити всі спроби примирення між Тайбей і Пекіном.

З урахуванням подій минулого для вирішення тайванського питання у КНР розробили курс «Мирне об'єднання та одна держава – два лади». Його положення зводяться до наступного:

1. Принцип «одного Китаю» з центральним урядом у Пекіні.

2. Співіснування двох ладів – континентального соціалізму та острівного капіталізму.

3. Високий рівень самоврядування на Тайвані.

4. Мирні переговори як запорука об'єднання та співіснування.

Вплив КНР на Тайвань. До того як 1949 року на материку перемогла комуністична революція, у «Великому Китаї» правила націоналістична партія Гоміньдан на чолі з генералісимусом Чан Кайші. Військова поразка від Мао Цзедуна та його компартії змусила гоміданівців втекти на о. Тайвань. Сьогодні керівництво КНР дотримується курсу відходу від явної політичної конфронтації (як це було раніше) через її недоцільність. Насамперед це обумовлено двома факторами.

Перший (економічний). Китай давно співпрацює з Тайванем у економічній сфері. За останні 30 років спостерігалося значне зростання товарообігу між Пекіном та Тайбеєм.

Другий (політичний). Незалежність Тайваню визнана деякими державами, що розвиваються, і неофіційно підтримується низкою світових держав. У зв'язку з цим ескалація воєнного конфлікту може викликати широкий міжнародний резонанс і залучити Пекін до конфронтації з країнами Заходу, і насамперед із США. Однак китайське керівництво не соромиться демонструвати свою військову міць і періодично «нагадує» Тайваню, що у разі вирішення проблеми силовим методом шансів біля острова залишитись незалежним небагато. Виходячи з цього, сьогодні обидві сторони наголошують на веденні інформаційної війни, яка, по суті, і не припинялася з 1949 року.

«Хакерські угруповання з материкового Китаю протягом тривалого часу зламували адміністративні установи та їх провайдери», – сказав заступник голови тайванського управління з розслідування кіберзлочинів Лю Цзяжун. За його словами, метою хакерів були важливі документи та інформація.

Серія атак розпочалася у 2018 році, проте спецслужби Тайваню не змогли визначити, які дані були вкрадені, оскільки хакери приховали свої сліди. Серед компаній, які зазнали атаки, були щонайменше чотири тайванські технологічні фірми, які надавали інформаційні послуги владі Тайваню. За словами Лю Цзяжуна, дві причетні до атак хакерські групи Blacktech і Taidoor діяли за підтримки Комуністичної партії Китаю. Хакери намагалися знайти лазівки у системах постачальників інформаційних послуг.

У ситуації, що склалася, інформаційно-психологічний вплив (ІПВ) є одним з ефективних способів тиску Пекіна на військово-політичне керівництво Тайваню, населення та збройні сили острова, а також потужним інструментом формування світової громадської думки на свою користь.

В цілому при наданні ІПВ на Тайвань Китай ставить перед собою такі завдання:

1. Вплинути на громадську думку як у самому Тайвані, так і у світі щодо необхідності об'єднання країни, тобто возз'єднання одного народу під одним державним прапором.

2. Створити в очах світової спільноти образ тайванського уряду як «сепаратистського».

3. Дати зрозуміти, що існує можливість вирішення тайванської проблеми силовими методами, у разі реалізації якої Тайбей приречений на поразку.

4. Показати прагнення Пекіна до дипломатичного процесу примирення та об'єднання за одночасної протидії керівництву Тайваню цьому процесу.

Органи пропаганди та інформаційної війни КНР. Слід зазначити, що вирішенням перших двох завдань на стратегічному рівні займаються переважно державні органи та установи. Зокрема, за даними зарубіжних ЗМІ, на даний час у Китаї створено потужну державну систему ведення інформаційного протиборства, яка дозволяє здійснювати масоване ІПВ на противника як у мирний, так і у воєнний час.

Науковим ядром системи є дослідницьке бюро при Держраді (уряді) КНР та системно-аналітичний центр міністерства державної безпеки (МДБ). Як теоретична база використовуються рекомендації та розробки Академії військових наук Народно-визвольної армії Китаю (НВАК).

У самій НВАК завдання ІПВ на оперативно-тактичному рівні вирішують політичні органи під керівництвом головного політичного управління (ГПУ) армії. Головне політичне управління є найвищим керівним органом, який відповідає за партійну та ідейно-політичну роботу в збройних силах Китаю. Партійні структури є у всіх частинах та з'єднаннях НВАК. Без підпису політкомісара жоден наказ, зокрема бойовий, не має сили. До складу ГПУ входять у тому числі управління пропаганди та агітації, у зв'язках із громадськістю, а також видавництво газети «Цзефанцзюньбао» та інші підвідомчі установи: народно-революційний військовий музей Китаю, кіностудія «1 серпня» тощо. Завданням цього органу є також розробка основних методів ведення зовнішньополітичної пропаганди у час.

У структурі генштабу НВАК питаннями психологічної війни займається окреме технічне управління, відоме як третє управління. Воно координує роботу інформаційних служб розвідки та веде моніторинг телекомунікацій армій противника, забезпечує ГШ інформацією, що базується на зібраному матеріалі військового характеру, проводить радіо- та радіотехнічну розвідку. Найбільш досконалі китайські системи збору інформації базуються на гірських районах Китаю,

і навіть на островах, здійснюючи покриття країн Азіатсько-Тихоокеанського регіону (АТР). З кінця 90-х років минулого століття подібними системами оснащуються і кораблі військово-морських сил НВАК.

Цензура як контрпропаганда. Особливого значення у КНР приділяється питанням контрпропаганди та протидії ІПВ із боку Тайваню. З цією метою ведеться тотальний контроль за ЗМІ країн Тихоокеанського регіону, а в Китаї іноземні засоби масової інформації заборонені на офіційному рівні. При цьому канали, які свого часу встигли отримати ліцензію на мовлення закордонних ЗМІ (BBC, CCN), піддаються жорсткій цензурі. Заборонено підписку та продаж світового друку, який не пройшов перевірку.

Міністерство культури КНР випустило спеціальну постанову, згідно з якою всі національні радіо- та телестанції не можуть надавати ефірний час закордонним компаніям, а також вести з ними спільне мовлення. Крім того, заборонено участь іноземців у програмах, що виходять у прямому ефірі або на регулярній основі. Для інших видів співпраці з вищезазначеними компаніями необхідно отримати дозвіл у місцевих відділеннях міністерства.

У той же час у Китаї з кожним роком зростає кількість інтернет-користувачів, що створює все більше проблем для органів нагляду. Місцеві спецслужби ретельно відстежують користувачів, які відвідують заборонені сайти. Зокрема, їх цікавлять ті, хто набирає у пошукових системах слова «Тайвань», «права людини», «дисидент», «демократія» тощо.

Влада країни за допомогою цезури не допускає, щоб громадяни Китаю виходили у своїх дискусіях за межі дозволеного. Інтернет-поліцейські в режимі реального часу контролюють та спрямовують дискусії на форумах та блогах. При цьому користувачам з КНР відкрито лише одну пошукову систему – національну Baidu, а до таких ресурсів як Google, Yahoo, Bing тощо, доступ обмежений.

У червні 2011 року для захисту інформаційних ресурсів керівництво республіки ухвалило рішення щодо створення спеціального підрозділу з протидії кібератакам. За словами китайських чиновників, мета всіх цих кроків – «захистити національну інтелектуальну власність та гарантувати першість держави у культурній сфері».

Насправді ж поставлені такі завдання: не допустити пропаганди з-за кордону (зокрема, з Тайваню), маніпулювати громадською думкою, а також висвітлювати світові та внутрішні події під кутом, вигідним керівництву країни. Керівництво КНР приділяє особливу увагу ЗМІ. Зокрема, за даними китайської преси, лише за останні кілька років на зовнішньополітичну пропаганду було виділено понад 80 мільярдів доларів.

Центральне інформагентство Китаю Сіньхуа організувало цілодобову телевізійну службу новин англійською зі штаб-квартирою в Нью-Йорку. Державні ЗМІ вже розмістили близько 400 своїх кореспондентів у понад 117 зарубіжних корпунктах. Ці заходи було вжито з метою сформувати у закордонної аудиторії прокитайську думку на вирішення тайванської проблеми.

Демонстрація військової сили КНР. Аналіз методів ІПВ Китаю на населення Тайваню показує, що до найефективніших з них належать: використання емоційного фактора, факторів сенсаційності та терміновості, методу неодноразового повторення інформації, подання «потрібної» інформації та тиску військовою потужністю. У моменти загострення відносин із Тайванем Пекін робить ставку саме на останній метод.

Демонстрація військової техніки, участь у виставках – продажах зброї та регулярне проведення навчань – все це є елементами попередження Тайбея про можливі для нього наслідки. Вони особливо ефективні щодо Тайваню, оскільки острів вразливий для ракетних атак з боку КНР, а протиракети американського виробництва «Петріот» ПАК-2 зосереджені в окрузі Тайбея, залишаючи Тайчжун і Гаосюн – два інші найбільші міста, фактично без захисту.

У висновку, хочеться відзначити, що «тайванське питання» в американо-китайських відносинах завжди грало значну роль протягом свого існування. Проте, незважаючи на те, що «тайванська проблема» багато в чому взаємозалежна від політики КНР, американська зовнішня політика щодо Тайваню проводилася відповідно до своїх принципів, які не належали до Китаю. Сьогодні, Тайвань є цілком сформована самостійна політична одиниця, яка за своїм строєм багато в чому відрізняється від свого геополітичного сусіда. І якщо найближчим часом відбудеться

військове зіткнення Китаю і Тайваню, то передбачити дії США буде досить складно через тонкі дипломатичні відносини США-Китай і США-Тайвань. Але загальновизнаним фактом серед аналітиків є те, що виникнення подібної ситуації може призвести до введення миротворчих сил, і тому головним завданням у найближчій перспективі має стати недопущення подібного виходу в майбутньому.

Можливий прогноз розвитку подій. В травня 2022 року загострився конфлікт між США та Китаєм через частково визнаний Тайвань.

23 травня президент США Джо Байден оголосив про те, що його країна повністю підтримає Тайвань і стане на її захист у разі початку китайської військової операції, чутки про проведення якої ходять вже давно. Міністерство закордонних справ Китаю у досить жорсткій манері відповіло владі США – МЗС закликали американців бути обережними у висловлюваннях та діях.

Китай здатний захопити Тайвань у разі спроби силового вирішення питання непідконтрольного йому острова, проте навіть можливий успіх дістанеться йому дорогою ціною, вважають аналітики CNN.

Автори видання вказали, що Китай перевершує Тайвань за кількістю військ та озброєння, включаючи тих, які могли б надати союзники острова, зокрема США та Японія. Це означає, що якщо Китай сповнений рішучості захопити острів, він, ймовірно, зможе це зробити, але захоплення відбудеться надзвичайно «кривавою» ціною для Пекіна, кажуть вони. Аналітики вважали подібне вторгнення небезпечнішим і складнішим, ніж висадка союзників у Нормандії під час Другої світової війни.

Експерти CNN також оцінили морський, повітряний та наземний варіанти китайського вторгнення. Вказується, що Китай має найбільший у світі військово-морський флот (близько 360 бойових кораблів) і може використовувати найбільший цивільний флот для перекидання військових та зброї. Проте для успіху Народно-визвольна армія Китаю (НОАК) повинна буде перекинути тисячі танків, знарядь, бронетранспортерів через Тайванську протоку шириною близько 180 кілометрів, що буде «довгою і небезпечною місією, під час якої кораблі будуть легкою здобиччю»,

оскільки Тайвань має великий запасом протикорабельних ракет, отриманих від США та вироблених на острові.

На думку Говарда Уллмана, колишнього офіцера ВМС США, така операція займе кілька тижнів, і, незважаючи на морську міць Китаю, йому просто не вистачить військового потенціалу та можливостей для повномасштабного десантного вторгнення на Тайвань у найближчому майбутньому. Він вважав, що Китаю знадобиться понад 1,2 мільйона військових. При цьому Китай може також вирішити, що втрати того коштуватимуть.

Зазначається, що Китай за рахунок майже 1600 бойових літаків матиме перевагу і в повітрі, до чого, швидше за все, прагнутиме на ранній стадії конфлікту. Тайваню тут готові допомогти поставлені Сполученими Штатами зенітні ракети Stinger та системи ППО Patriot. Крім того, протягом останніх трьох років острів вклав значні кошти у виробництво власних ракет. З іншого боку, зазначають аналітики, Китай матиме перевагу перед США через свою близькість до Тайваню. На думку американських військових, повітряний конфлікт тут може зайти в глухий кут.

Наземна операція НВАК складна тим, що Китаю необхідно буде знайти підходяще місце для висадки, а Тайвань чудово знає їх і давно спорудив там оборонні укріплення. Десант із повітря малоймовірний, як стверджують аналітики, через відсутність десантників у НВАК. Ще однією проблемою для китайських військ буде відсутність у них бойового досвіду. При цьому наголошується, що й війська Тайваню не мають такого.

Нарешті, ще одним варіантом дій Китаю називається захоплення віддалених тайванських островів або взяття під контроль повітряних та морських кордонів Тайваню та блокаду острова за рахунок цього. У такому разі Китай може заблокувати та конфіскувати військову допомогу від США як порушення суверенітету країни. Уряду Тайваню дозволять функціонувати у звичайному режимі. Цей варіант, вважають CNN, мав би перевагу для Китаю в тому, що м'яч у питанні про застосування сили для зняття блокади був би на стороні США.

За підсумками, як вважає директор азіатської програми Німецького фонду Маршалла в США Бонні Глейзер, китайське вторгнення на Тайвань є малоймовірним.

На його думку, у НВАК немає повної впевненості в тому, що вона може захопити та контролювати Тайвань.

Але найбільша загроза сьогодні – не висадка військ на берег, а спроби непримиренних опонентів використати відкритість суспільств та мереж. Кіберзагрози вважають найбільш значним ризиком. Зловмисники КНР намагаються підірвати політичну владу, поставити під загрозу критичну інфраструктуру та завдати збитків фінансово-торговельній галузі.

В свою чергу, у боротьбі за захист Тайваню беруть участь посадовці країн, включаючи Австралію, Індонезію, Японію. Тренування будуть проводяться за допомогою спеціального американського симулятора міжнародних комп'ютерних атак, що використовується в навчаннях CyberStorm раз на два роки.

3.2 Інформаційна безпека держав в контексті боротьби з транснаціональними інтернет-гігантами США

Сьогоднішнє протистояння двох світових держав стало, по суті, першою відкритою сутичкою, в якій зійшлися модель «класичного» західного (або ринкового, називайте, як хочете) капіталізму і та, яку вибрав для себе, що розвивається небаченими темпами, що сповідує зовсім інші правила та закони Комуністичний Китай. Зараз світ опинився на порозі нового переділу, але не військово-політичного, а інформаційно-безпекового, де головними гравцями будуть уже не тільки держави та навіть не блоки країн, а провідні транснаціональні корпорації найбільших промислово розвинених держав.

Події, що розгортаються навколо двох держав – США та Китаю, природно далекі від повномасштабної «битви», проте самі закони людської природи диктують необхідність приготувань до можливого зіткнення. Інформаційні технології, у найширшому розумінні цього словосполучення, для досягнення стратегічної переваги у XXI столітті відіграють роль як ніколи важливу.

ТНК – це насамперед інформаційна безпека та майбутнє цифрового розвитку країни. ТНК є сукупністю розташованих на територіях кількох держав, у

різноманітній мірі легалізованих та організаційно оформлених економічних суб'єктів, об'єднаних управлінням з єдиного центру (центрів) та містить набір загальнозначущих інтересів стратегією розвитку, реалізація якої об'єктивно необхідна для підтримки їх конкурентоспроможності у глобальному масштабі та можлива мірою лише завдяки безпосередній та диверсифікованій участі даних суб'єктів у політичних інститутах, відносинах та процесах на макро- та мікрорівні, що має великий вплив на ІБ держав.

Небезпека подібної тіньової політичної практики ТНК для держави полягає, насамперед, у тому, що вони здатні впливати на державну владу, не вступаючи з нею у відкритий конфлікт, а просто підміняючи державні інтереси власними. Часто це зумовлено гіпертрофованою роллю в економіці країни того чи іншого сектора, що може спричинити феномен «банановых республік», де політичні процеси контролюються іноземними компаніями.

Іншими словами, можна сказати, що система відносин між державою та ТНК є діалектичною єдністю протиріч. З одного боку, ТНК є важливим інструментом зовнішньоекономічного та зовнішньополітичного впливу, і держава не може не використати це на користь свого затвердження на світовій арені. З іншого боку, єдність інтересів не виключає наявність суперечностей.

В країнах базування своїх філій ТНК використовують переважно нелегальні та нелегітимні методи впливу на національні уряди. Будучи тісно пов'язаними з місцевими групами, які отримують вигоди від іноземних капіталовкладень, вони можуть використовувати власні або партнерські компанії для підтримки певної суспільно-політичної сили, що виступає за вигідні ТНК реформи, що підриває інформаційну безпеку держави. Тобто, перетворившись із суб'єкта виключно економічної діяльності на суб'єкт політики, ТНК є інструментом інформаційної безпеки держави.

Загострена, особливо зараз, діяльність уряду США з обмеження співпраці з «ворожими» компаніями, начебто, не викликає особливого подиву. Однак тут є нюанси. Корпорації: Apple і Google, Huawei і Xiaomi, як і багато інших, будучи формально китайськими та американськими фактично є приватними акціонерними

товариствами. Оперуючи багатомільярдними прибутками, проникаючи в повсякденне життя сотень мільйонів рядових користувачів гаджетів і ПЗ по всьому світу, будучи інструментом просування ідей і товарів вони вийшли за межі національних держав, перетворившись на транснаціональні конгломерати, що вже в свою чергу зробило їх заручниками власного успіху. Склалася досить парадоксальна ситуація, маючи на даний момент прообраз єдиної світової економіки, об'єднаного Інтернетом без кордонів та паспортів IT-спільноти, ми все ще знаходимося у світі національних урядів, що конкурують за сфери впливу. В умовах відносин між США і Китаєм економіка, науковий прогрес став розмінною монетою геополітики.

Від союзників, за часів Другої світової війни, до прямих бойових зіткнень у Кореї, від спільного протистояння розширенню впливу СРСР в Азії, до стану, що все більше нагадує холодну війну між Сполученими Штатами і колись Країною Рад. На тлі «гойдалки» зовнішньополітичного курсу Піднебесної, розвиток її IT сектору також переживав не найкращі часи. Свої перші ЕОМ китайці отримали лише наприкінці 50-х років XX століття, за загального сприяння північних товаришів. Скопіювавши радянські моделі комп'ютерів М-20 і БЭСМ-2, не маючи власного повного циклу з розробки, створення, впровадження, модернізації передових обчислювальних систем, в умовах планово-командної економіки, розвиток комп'ютерної індустрії в країні на цьому етапі закінчився із припиненням кооперації з СРСР . Звинувативши 1961 року КПРС «зрадниками та ревізіоністами», послідовники секретаря Мао в той же час втратили матеріально-технічну підтримку з Союзу. Оскільки до потепління відносин із «заходом» залишалося ще більше 10 років, а країна «Культурна революція», яка ввела в перманентний хаос, також явно не сприяла становленню далекого від потреб робітничо-селянської країни напряму розвитку ЕОМ, то ще якихось 30-40 років. тому IT у Китаї перебувало в зародковому стані.

Прорив у міжурядових взаєминах Америки та Китаю для останнього став першим щаблем до тих висот у IT-секторі яких Піднебесна досягла сьогодні. Нестримне зростання Китаю тривалий час підігрівалося «західною» спільнотою, але часи змінилися. Складно сказати, що КНР при Великому Кормчому Мао Цзедуні була

більш миролюбною і толерантною, демократичною і відкритою країною, ніж її сучасна версія, проте те, що ми можемо спостерігати у відносинах, між ще недавно теплими партнерами.

З погляду керівництва США, такі популярні ТНК, як Twitter та Youtube, забезпечують свободу слова та самовираження, у той час як для Пекіна вони виступають у ролі інструментів інформаційного впливу, нав'язування західних цінностей. У 2007 році Китай вперше заблокував відеохостинг Youtube для захисту ідеологічної стабільності всередині держави, а остаточно сайт був заблокований для китайських користувачів у 2009 р. Паралельно загострюється конфлікт між Китаєм та пошуковою системою Google. Розбіжності між компанією та китайським керівництвом виникли з питань цензури, на якій наполягало останнє. Ідеологія Google повністю суперечить принципам китайського режиму; Пекін вважає, що цензура та державне регулювання кіберпростору не є порушенням прав і свобод людини, а, навпаки, спрямована на їхній захист.

В протидію транснаціональним корпораціям США, у січні 2010 року – новий скандал. Все почалося з того, що у грудні 2009 року китайські хакери здійснили атаку на поштовий сервіс компанії. Зловмисникам вдалося зламати поштові скриньки кількох китайських правозахисників та отримати доступ як мінімум до заголовків електронних листів постраждалих користувачів. Представники корпорації заявили, що кібератака була продуманою і відбувалася з конкретними цілями. Атаку зазнали як мінімум 20 компаній та приватні користувачі.

Авторитетні китайські джерела публічно не називають транснаціональні інтернет-гіганти США як перевірене джерело основних типів загроз ІБ. Хоча представники МЗС зазначають, що «кібератаки проти Китаю в основному відбуваються зі сторони США» (на що вказує явне місце розташування IP-адреси зловмисника). Наприклад, представник міністерства закордонних справ, перераховуючи кількість кібератак, яких зазнав Китай у 2021 році, заявив: «Атаки, які відбуваються зі Сполучених Штатів, займають перше місце серед цих хакерських дій», що однозначно ставить під загрозу ІБ держави.

Тим часом у країні з'явилися свої місцеві аналоги найбільших інтернет-гігантів США, задля забезпечення своїх інтересів та інформаційної безпеки держави. Наприклад, Китай – чи не єдина країна світу, в якій лідером ринку інтернет-пошуку є зовсім не Google, а місцевий проект Baidu. Те саме стосується й ринку соціальних мереж. Назви WeChat, Weibo, TikTok, Renren, QQ та YouKu нічого не скажуть європейцю чи американцю, але у Китаї це мегапопулярні соціальні сервіси з величезною аудиторією. Порівняння зазначене на рисунку 3.1.

Рис. 3.1 Дані China Internet Report із порівнянням західних та китайських сервісів.

У свою чергу, КНР також спричиняли неабиякий влив на ІБ США. Спочатку позбавивши китайські телефони підтримки сервісів від Google, уряд США розгорнув справжню компанію з дискредитації корпорації Huawei. Висунуті колишнім президентом США Трампом звинувачення в тому, що Huawei та ZTE передає персональні дані користувачів китайським спецслужбам, були лише черговим кроком по відсіченню компаній від участі в освоюванні бюджетів телекомунікаційних гравців ринку зі створення швидкісних інтернет мереж 5G. Президент США своїм указом про заборону використання обладнання, що становить загрозу національній безпеці США, поставив китайську компанію Huawei у складну ситуацію.

У січні 2003 року компанія Cisco звинуватила Huawei у порушенні своїх патентів та незаконному копіюванні операційної системи Cisco IOS та інтерфейсу командного рядка. У позові вказувалося, що Huawei скопіювала вихідні коди, документацію Cisco та інші матеріали, захищені авторським правом. Американська компанія зажадала не лише припинити використання її інтелектуальної власності, а й відшкодувати збитки, отримані внаслідок незаконних дій. У червні того ж року американський суд визнав Cisco постраждалою стороною. І в той же час, суддя відмовився повністю забороняти використання програмного забезпечення Huawei для мережевого обладнання.

2004 року виник новий конфлікт. Стало відомо про лист керівництва Fujitsu Network Communications генеральному директору Huawei. У ньому йшлося про співробітника китайської компанії, Йі Бін Чжу (Yi Bin Zhu), який ретельно вивчав електронні компоненти пристрою, випущеного Fujitsu для операторів зв'язку. У цьому не було б нічого незвичайного, якби співробітник не розібрав цей пристрій прямо на торговій виставці, де Fujitsu демонстрували відвідувачам. Спійманий зізнався, що він фотографував компоненти. На бейджі шпигуна значилося, що він працює на компанію Weihua, але в кишені виявилася візитівка, де значилося, що людина – співробітник Huawei. Представники останньої заявили, що нічого не знають ні про цю людину, ні про її наміри.

У 2008 році уряд США звинуватив китайські компанії Huawei і ZTE в тому, що вони становлять загрозу безпеці Америки. Повідомлялося, що обладнання цих

компаній використовують військові США, державні організації, наукові установи та корпорації, які «зливають» інформацію по Мережі до Китаю. Тому військовим та чиновникам США заборонили купувати обладнання з КНР, а Huawei та ZTE втратили можливість купувати американські стартапи.

Виділяючи інформаційний аспект діяльності транснаціональних інтернет-гігантів та їхнього впливу на інформаційну безпеку країни необхідно звернути увагу на ідеологію цих організацій. Інструментом реалізації політики та ідеології виступають в інформаційному суспільстві телекомунікаційні структури. Серйозну шкоду психічному здоров'ю населення завдає ринок мас-медіа, який заповнений аудіо та відео продукцією, що містить елементи моральної та культурної деградації (пропаганди наркотиків, сцени жорстокості тощо). Важливу роль у цьому відіграють західні ЗМІ та ТНК, що реалізує програму пропаганди моди на вживання шкідливих для здоров'я людини продуктів харчування, зокрема алкоголю та тютюну. Звичайно, політика ТНК в інформаційній сфері багато в чому регулюється їхніми власними економічними інтересами, проте не можна категорично відкидати можливість впливу на інші країни за допомогою ТНК таких сил як інтереси бізнес-груп і дії спеціальних служб з формування громадської думки. Наприклад, у стінах ЦРУ та Тавістокського інституту США було розроблено проект "MK-ULTRA". Основна мета проекту – зміна свідомості населення в сторону власних економічних, політичних цілей.

Вплив транснаціональних інтернет-гігантів США на інформаційну безпеку КНР є значним, адже саме ТНК у суспільстві багато в чому виконують світоглядну функцію, формуючи в людей систему поглядів на людський світ і місце в ньому людини, ставлення людини до навколишньої соціальної дійсності і до самого себе, а також обумовлені цими поглядами життєві позиції людей, їх ідеали та потреби.

ВИСНОВКИ

Отже, поняття інформаційної безпеки пройшло низку етапів та виникло ще до початку XIX століття; воно багатогранне і характеризується безліччю складових. Виходячи з цього, можна говорити про велике значення ІБ в сучасному світі. Інформаційні технології стрімко розвиваються, прогрес не стоїть на місці, постійно з'являються нові технології, які зумовлюють появу нових підходів і теоретичного обґрунтування загалом, розробляють нові методи захисту інформації.

Досліджувані США та КНР мають принципово різні підходи до управління інформаційної безпеки усередині країн. Сполучені Штати трактують ІБ з позиції гарантій населенню доступу до інформації. Захист громадянських свобод і права на приватне життя залишаються фундаментальними цілями в практично всіх законодавчих актах США, що видаються, що зачіпають політику в інформаційно-безпековому просторі. У Китаї ж керівництво країни в процесі формування політики в галузі ІБ приділяє увагу зростаючій ролі інтернету, взаємозалежності країн у глобальному кіберпросторі, а також можливим загрозам, тому бачить необхідність контролю внутрішнього інтернету і здійснює його.

Керівництва країн вживають заходів щодо захисту своїх даних в інформаційній мережі, формуються системи забезпечення кібербезпеки. Інституційний аспект забезпечення ІБ в США відрізняється своєю трирівневою системою, що дозволяє діяти кожній структурі автономно, при цьому дотримуючись загальної стратегії. У китайській системі забезпечення необхідно виділити інтеграцію військових та цивільних структур, модернізацію НВАК, націлену на розвиток інформатизації та покращення взаємодії всіх структур під час проведення спільних операцій.

Розглянувши законодавчі бази США та КНР у галузі ІБ, стає ясно, що і Китай, і Сполучені Штати, усвідомлюють зростаючу роль інтернету, необхідність у впровадженні кібербезпеки у всі інформаційні структури, та докладають зусиль, щоб зміцнити не лише свою національну інформаційну безпеку, а й зробити внесок у розвиток норм регулювання міжнародного ІБ-простору.

Проаналізувавши Тайванську проблему та протистояння КНР транснаціональним інтернет-гігантам США в ІБ-просторі, стає ясно, що між країнами існує протистояння, яке стало продовженням політичних розбіжностей в інших сферах. Рівень розвитку інформаційних технологій в обох країнах чинить взаємний тиск США та КНР, створюючи кіберзагрози в діапазоні відносин, що стосуються і політичних, і ділових, та економічних інтересів. Це робить китайсько-американський діалог у питаннях ІБ ще більш актуальним та важливим. Незважаючи на складність прийняття спільних рішень для США та КНР, країни все ж таки йдуть на контакт і проводять зустрічі різних рівнів, підписують спільні угоди, усвідомлюючи важливість такої спільної сфери, як ІБ-простір, та визнаючи наявність спільних загроз.

В процесі дипломної роботи були досягнені всі цілі та розкрита мета, а саме – визначено сутність та особливості поняття інформаційної безпеки держав, їх проблеми та перспективи в умовах конфліктної взаємодії США та КНР.

У теоретичній частині викладено передумови формування та теоретичні підходи поняття «інформаційна безпека», методи та інструменти захисту ІБ держав світу, цілі та задачі США та КНР на міжнародній арені.

Практичний розділ містить стратегію ІБ США та КНР в контексті регулювання Тайванської проблеми та боротьби з транснаціональними інтренет-гігантами США.

Метод порівняльного аналізу був застосований до нормативно-правової бази США та КНР у сфері ІБ та дозволив виявити особливості забезпечення ІБ у досліджуваних країнах, позначити їх спільні інтереси. Історичний метод був використаний задля виявлення передумов виникнення поняття «інформаційна безпека» та його розвитку. Системний метод дозволив комплексно підійти до розуміння проблем ІБ відносно держав та їх перспектив на міжнародному рівні та аналізі розвитку інституційного аспекту забезпечення ІБ у Китаї та США.

Отже, можна зробити висновки, що ескалація китайсько-американських суперечок у питаннях ІБ стимулює зростання напруженості в кіберпросторі в цілому та провокує подальше втягування в гонку інформаційної безпеки усієї світової спільноти. Від кооперації чи суперництва навіть Китаю у цій сфері також залежить ІБ

країн, які мають менш значними можливостями даному просторі. Саме тому тема диплому є і буде залишатися актуальною, адже саме США та КНР вважаються одними з найвпливовіших акторів світової політики, а їх взаємодія в питаннях ІБ та стабільність системи взаємовідносин, що формується ними, мають глобальне значення.

СПИСОК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Антипов К. Кіберконфлікт у китайсько-американських відносинах та пошуки діалогу // Проблеми Далекого Сходу. - 2013. - №6. - С. 39-54.

2. Антоніна Буравкова. Американсько-китайські відносини в постбіполярну епоху: глобальний і регіональний вимір. URL: https://ipiend.gov.ua/wp-content/uploads/2018/08/buravkova_amerykansko.pdf (дата звернення: 13.05.2022)

3. Бармен Скотт. Разработка правил информационной безопасности. М. Вильямс, 2002. — 208 с.

4. Бергер Я. Велика стратегія Китаю в оцінках американських та китайських дослідників// Проблеми Далекого Сходу. - 2006. - №1.

5. Бжезинский З. Велика шахівниця: панування Америки та його геостратегічні імперативи. Переклад О. Ю. Уральської / Збігнєв Бжезінський. - М.: Міжнародні відносини,1999. – 256 с.

6. Боднар І.Р. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. С. 68–75.

7. В. Пашков. Інформаційна безпека США. Зарубіжний військовий огляд № 10/2010, стор. 3-13.

8. Відносини КНР та США в інтернет-просторі в контексті забезпечення кібербезпеки. URL: https://www.gramota.net/articles/issn_1997-292X_2014_12-3_31.pdf (дата звернення: 17.05.2022)

9. Волошин Ю.О. Legal globalization and interstate integration as a leading factor of the formation of state security and sovereignty. Atlantic Press. 2nd International Conference on Social, Economic and Academic Leadership . – 2018, № 11. – P. 351-358.

10. Галія Ібрагімова. Стратегія КНР в області управління інтернетом і забезпечення інформаційної безпеки. URL: http://docplayer.com/25816967-Galiya-ibragimova-strategiya-knr-v-oblasti-upravleniya-internetom-i-obespecheniya-informacionnoy-bezopasnosti.html (дата звернення: 21.05.2022)

11. Глобальний виклик транснаціональних корпорацій. URL: https://zn.ua/foreign_economics/globalnyy_vyzov_transnatsionalnyh_korporatsiy.html (дата звернення: 15.05.2022)

12. Д. Устинов. Сутність інформаційної безпеки. URL: https://cyberleninka.ru/article/n/suschnost-informatsionnoy-bezopasnosti/viewer (дата звернення: 19.05.2022)

13. Еволюція політики КНР в сфері інформаційної безпеки. URL: https://cyberleninka.ru/article/n/evolyutsiya-politiki-knr-v-oblasti-informatsionnoy-bezopasnosti/viewer (дата звернення: 14.05.2022)

14. Еволюція політики КНР в сфері інформаційної безпеки. URL: https://www.imemo.ru/files/File/magazines/puty_miru/2020/01/07_Romashkina.pdf (дата звернення: 22.05.2022)

15. Єдиний Китай та провокації США: історія тайванського питання. URL: https://ren.tv/longread/963748-ostrov-nevezeniia-pochemu-na-taivane-obostrilsia-konflikt-kitaia-i-ssha (дата звернення: 14.05.2022)

16. Зовнішньополітичні цілі та ідеологія. URL: https://studme.org/1405100329652/politologiya/vneshnepoliticheskie_tseli_ideologiya_kitaya (дата звернення: 23.05.2022)

17. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

18. Зубок М.І. Інформаційна безпека в підприємницькій діяльності. К. : ГНОЗІС, 2015. 216 с.

19. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Гуманітарні візії. 2016. № 2(1). С. 27–32.

20. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис. доктора юрид. наук : 12.00.07. Одеса, 2004. 427 с.

21. Кошурнікова Н.А. Особливості інформаційної політики сучасного Китаю // Китай: історія та сучасність: матеріали IX Міжнародної науково-практичної конференції, 2016. – 279-284.

22. Лінь Явен. Політика КНР щодо проблеми в Тайвані. URL: https:// politika-knr-v-otnoshenii-problemy-tayvanya-v-xxi-veke.pdf (дата звернення:16.05.2022)

23. Луцкий М.Г. Исследование программных средств анализа и оценки риска информационной безопасности / Луцкий М.Г., Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Захист інформації. – 2011. – №3. – С. 97-108.

24. Луцкий М.Г., Иванченко Е.В., Казмирчук С.В. Базовые понятия управления риском в сфере информационной безопасности /. // Захист інформації. – 2011. – №2. – С. 86-94.

25. Луцкий М.Г., Иванченко Е.В., Корченко А.Г., Казмирчук С.В., Охрименко А.А. Современные средства управления информационными рисками // Защита информации – 2012. – No1. – С. 5-16.

26. Маковський І. Ю. Етапи становлення та значення інформаційної безпеки для ефективного функціонування підприємств, 2017. URL: https://conf.ztu.edu.ua/wp-content/uploads/2019/12/554.pdf (дата звернення: 17.05.2022)

27. Малюк А. А. Інформаційна безпека: концептуальні та методологічні засади захисту інформації, 2004. -280 с.

28. Микитенко Т.В., Петровська І.О., Рогов П.Д., Гаркуша А.О. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2014. № 1. С. 24–31.

29. Національна академія СБУ. Стратегічні комунікації в умовах гібридної війни: погляд від волонтера до науковця, 2021.

30. Основна зовнішньополітична мета США. URL: http://www.usapolitika.ru/osnovnaya-vneshnepoliticheskaya-cel-ssha-1.html (дата звернення: 22.05.2022)

31. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України. Політичний менеджмент. 2008. № 4. С. 135–141.

32. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. Юридичний журнал. 2009. № 5. С. 122–134.

33. Принцип одного Китаю та Тайванське питання. URL: https://www.mfa.gov.cn/ce/cgkhb//rus/zgzt/twwt/t118063.htm (дата звернення: 15.05.2022)

34. Системний підхід до формалізації поняття «Інформаційна безпека». URL: http://bses.in.ua/journals/2018/34_2018/52.pdf (дата звернення: 22.05.2022)

35. Соколовський М. США і Китай – гра тільки починається... / Михайло Соколовський // Дзеркало тижня. – 2001, 20–27 квітня.

36. Структура органів державної влади, які забезпечують інформаційну безпеку США. URL: https://intuit.ru/studies/courses/563/419/lecture/9576?page=2 (дата звернення: 14.05.2022)

37. Тайванська проблема. URL: https://kazedu.com/referat/121645/2 (дата звернення: 18.05.2022)

38. Тайванське питання. Внутрішні детермінанти. URL: https://cyberleninka.ru/article/n/tayvanskiy-vopros-vneshnie-i-vnutrennie-determinanty/viewer (дата звернення: 21.05.2022)

39. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 422 с, с. 379.

40. ТНК як фактор впливу США у Китаї. URL: https://vuzlit.com/20899/faktor_vliyaniya_kitae (дата звернення: 15.05.2022)

41. Ю.А. Гатчин, В.В. Сухостат. Теорія інформаційної безпеки та методологія захисту інформації, 2018. URL: https://books.ifmo.ru/file/pdf/2372.pdf (дата звернення: 18.05.2022)

42. A Theory on Information Security URL: https://www.researchgate.net/publication/318589055_A_Theory_on_Information_Security (дата звернення: 21.05.2022)

43. An official website of the United States Government. URL: https://www.state.gov/ (дата звернення: 20.05.2022)

44. Balakin, V.I. (2013). Taiwan in the system of East Asian integration China. In: China in world and regional politics. History and the present. Vol. XVIII. Moscow: IFES RAS, p. 223—231.

45. Chang A. Warring State. China's Cybersecurity Strategy. / A. Chang // CRYPTOME. ORG December, 2014. URL: https://cryptome.org/2014/12/chinas-cybersecurity-strategy-china-file-14-1205.pdf (дата звернення: 20.05.2022)

46. China and the United States. The Brookings Institution, Asia Working Group. Paper 1. URL: https://www.brookings.edu/wp-content/uploads/2016/07/taiwan-elections-china-us-implicationsbush-FINAL-2.pdf (дата звернення: 21.05.2022)

47. China vs Google, Facebook and other US internet giants: a lesson in internet oversight for the West. URL: https://www.scmp.com/comment/insight-opinion/article/2123957/china-vs-google-facebook-and-other-us-internet-giants-lesson (дата звернення: 22.05.2022)

48. Concepts of Information Security. National Academies of Sciences, Engineering, and Medicine. 1991. The National Academies Press. URL:https://doi.org/10.17226/1581 (дата звернення: 21.05.2022)

49. Goodman Peter S. Huawei Founder Ren Zhengfei Dismisses Chinese Military Connections. / Goodman Peter S. // International Business Times. 01.22.2015. URL: http://www.ibtimes.com/huawei-founder-ren-zhengfei-dismisses-chinese-military-connections-1791228 (дата звернення: 14.05.2022)

50. How Multinationals Can Withstand U.S.-China Trade Conflict. URL: https://www.winston.com/en/thought-leadership/how-multinationals-can-withstand-us-china-trade-conflict.html (дата звернення: 22.0.2022)

51. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron. China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, 2015. P 187-203.

52. Karl Maria Michael de Leeuw, Jan Bergstra. The History of Information Security: A Comprehensive Handbook 1st Edition. (October 16, 2007).

53. MacGregor A. China, U.S. making moves to implement cybersecurity agreements / A. MacGregor // The Stack.14.06.2016. URL:

https://thestack.com/security/2016/06/14/china-u-s-making-moves-toimplement-cybersecurity-agreements/United States Department of State (дата звернення: 21.05.2022)

54. Michael Cox, Doug Stokes. US Foreign Policy 3e, 2020.

55. Michael D. Swaine. Chinese Views on Cybersecurity in Foreign Relations. URL: https://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf (дата звернення: 16.05.2022)

56. Michael D. Swaine. Chinese Views on Cybersecurity in Foreign Relations. URL: https://carnegieendowment.org/email/South_Asia/img/CLM42MSnew.pdf (дата звернення: 17.05.2022)

57. Michael Lind. The American Way of Strategy: U.S. Foreign Policy and the American Way of Life, 2008.

58. Military and security developments involving the People's Republic of China 2021» (Annual Report to Congress by Office of the Secretary of Defense) URL: https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF (дата звернення: 22.05.2022)

59. Ministry of Foreign Affairs of the People's Republic of China. URL: https://www.fmprc.gov.cn/mfa_eng/ (дата звернення: 22.05.2022)

60. National Security Strategy of the United States of America / Seal of the President of the United States. December 2017 // The White House. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (дата звернення: 16.05.2022)

61. NCAFP. Cyberpower and National Security // American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy. 2013. V. 35. № 1. P. 45–58.

62. Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Prepared for the U. S.–China Economic and Security Review Commission by Northrop Grumman Corp.

63. Pillsbury M. China Debates the Future Security Environment / Michael Pillsbury. – Washington, DC : National Defense University Press, 2000. – 320 p.

64. Richard Weitz. China-US-Taiwan Scenarios in 2022. URL: https://www.chinausfocus.com/peace-security/china-us-taiwan-scenarios-in-2022 (дата звернення: 14.05.2022)

65. Robert Lai. Analytic of China Cyberattack. URL: https://www.researchgate.net/publication/267363551_Analytic_of_China_Cyberattack (дата звернення: 14.05.2022)

66. Rollins J., Henning A. C. Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations. / J. Rollins, A.C. Henning. URL: https://www.whitehouse.gov/files/documents/cyber/Congressional%20Research%20Service%20%20CNCI%20 (March%202009).pdf (дата звернення: 21.05.2022)

67. Shemchuk V. National Cyber Strategy of the United States of America. URL:http://elar.naiau.kiev.ua/bitstream/123456789/17521/1/%D0%9D%D0%92%204%2819%29_p119-124.pdf (дата звернення: 19.05.2022)

68. Sulmeyer Michael. Cybersecurity in the 2017 National Security Strategy / Michael Sulmeyer. // Lawfare. 19.12.2017. URL: https://www.lawfareblog.com/cybersecurity-2017-national-security-strategy (дата звернення: 17.05.2022)

69. The National Strategy for a New Century. – September 2002. – Washington : The White House. – 39 p.

70. The Taiwan Problem and China's Strategy for Resolving It. URL: https://mepc.org/speeches/taiwan-problem-and-chinas-strategy-resolving-it (дата звернення: 22.05.2022)

71. The World Factbook. URL: https://www.cia.gov/library/publications/the-world-factbook/geos/ ch.html (дата звернення: 21.05.2022)

72. U.S. Relations With Taiwan URL: https://www.state.gov/u-s-relations-with-taiwan/ (дата звернення: 20.05.2022)

73. Yulia Cherdantseva, Jeremy Hilton. A Reference Model of Information Assurance & Security. URL: https://ieeexplore.ieee.org/abstract/document/6657288/authors#authors (дата звернення: 22.05.2022)

ДОДАТКИ

Таблиця 2.1 Базові документи щодо забезпечення внутрішньодержавної інформаційної безпеки КНР

№	Назва документу	Рік впровадження	Основні положення
1.	Правила регулювання, забезпечуючи безпеку комп'ютерних та інформаційних систем	1994	Наділення Міністерства державної безпеки повноваженнями з контролю, інспекції та забезпечення національної ІБ, розслідування, розкриття та запобігання злочинам в області ІКТ.
2.	План державної інформатизації в рамках 9-го п'ятиріччя та перспективні цілі до 2010	1997	Позначення перспективних цілей ІБ, що передбачають інформатизацію всіх державних інфраструктур до 2010 р.
3.	Закон про безпеку мережевої інфраструктури та мережі Інтернет	1997	Заборона використання мережі для створення, розповсюдження, копіювання або передачі певних видів інформації, до яких віднесені заклики до невиконання або порушення державних законів, терористичної діяльності або порушення цілісності країни.

4.	Постанова Всекитайських зборів народних представників (ВСНП) про забезпечення безпеки в мережі Інтернеті	2000	Необхідність регулювання та моніторингу інформаційних відносин через значиму роль інтернету в економічному будівництві та інфраструктурі КНР.
5.	Постанова державної інформатизованої керівної групи щодо роботі в галузі зміцнення інформаційної безпеки.	2003	Необхідність зміцнення захисту критично важливої, стратегічної інфраструктури.
6.	Державна стратегія розвитку інформатизації на період з 2006 по 2020	2006	План створення структур регулювання діяльності в інформаційній сфері, виробництво власного програмного забезпечення, визначення базових векторів державної політики у галузі ІБ.
7.	Постанова Держради КНР щодо просування інформатизації та розвитку чинного захисту інформаційної безпеки	2012	- контроль над інтернет-додатками, віртуальними угодами у торговельно-економічній сфері, інформаційно-мовними послугами; - затвердження осіб, які відповідають за заходи щодо забезпечення безпеки у регіонах; - дозвіл застосування регіональною владою заходів щодо

			обмеження доступу до листування в інтернеті та інтернет-трафіку при виникненні загроз безпеці країни.
8.	Антитерористичний закон КНР	2015	- дешифрування інтернет-трафіку, застосування адміністративних заходів щодо вилучення у іноземних компаній та підприємств інформації при підозрі у її використанні для терористичних цілей; - запровадження цензури для діяльності новин на території КНР.
9.	Закон КНР про кібербезпеку	2016	Необхідність вказувати реальні дані користувача при реєстрації, обов'язкове зберігання інформації, що публікується, протягом 6 місяців на території КНР.
10.	Положення про захист безпеки критично важливої інфраструктури	2019	- захист критично важливої інформаційної інфраструктури від атак, вторгнень, втручання та знищення; - просування державою безпечних та надійних мережевих продуктів та послуг; - поліпшення стандартної системи мережевої безпеки.
11.	Заходи з приводу оцінки безпеки хмарних обчислень	2019	- введення відповідних заходів контролю при закупівлі та використанні продуктів, включених

			до каталогів спеціального мережевого обладнання безпеки; - запровадження більш високих вимог безпеки для хмарних обчислень, які використовуються державними установами та операторами зв'язку.
12.	Закон про шифрування даних	2020	- заборона порушення конфіденційності даних; - необхідність вжити заходів у разі виникнення загроз інформаційній безпеці.
13.	Закон КНР про безпеку даних	2021	Спрямовано регулювання відносин, що з обробкою даних. У новому економічному п'ятирічному плані наголошується на необхідності посилення впливу уряду на дані приватних компаній.